

U.S. Department
of Homeland Security

United States
Coast Guard



The **COAST GUARD** Journal of Safety
& Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council

Winter 2011–2012

Enhancing Global Supply Chain Security



**Innovative,
cooperative, and
sustainable measures**

Also inside:
Lessons Learned
from USCG Casualty Reports

PROCEEDINGS



Winter 2011–2012

Vol. 68, Number 4

Defining the Supply Chain

Defining the Supply Chain

- 6 **The Secure Chain**
by Mr. Anthony Barone
- 11 **The Coast Guard and Customs and Border Protection Partnership**
by LCDR Dan Somma and Ms. Jen Climenhaga
- 16 **The National Strategy for Global Supply Chain Security**
by Ms. Maranda Sorrells, Mr. Michael Callahan and Mr. Sean Moon
- 21 **The DHS Secure Supply Chain Initiative**
by Mr. Sean Moon, CAPT Kevin Kiefer and Ms. Kemba Walden

International Supply Chain Security

International Supply Chain Security

- 27 **International Maritime Organization User Guide**
by CAPT Kevin Kiefer and Mr. Marc Mes
- 29 **The Asia-Pacific Economic Cooperation**
by Mr. Sean Moon
- 34 **International Port Security**
by LT Dan Orchard

Information Sharing

Information Sharing

- 39 **Notice of Arrival and Departure**
by LT Sharmine Jones
- 42 **Keeping Cargo Moving**
by Captain Jeremy Sykes and Mr. Ed Merkle
- 45 **AIS in Action**
by Mr. Jason Tieman

Domestic Supply Chain Security

- 49 **Securing Certain Dangerous Cargoes**
by Mr. Bob Reimann and Mr. Mark Johnson
- 52 **Multi-Agency Strike Force Operations**
by LCDR Kevin Lynn
- 55 **Los Angeles Port Police**
by Mr. George Cummings
- 58 **Area Maritime Security Plans**
by Mr. Michael Smith

Domestic Supply
Chain Security

MTS Resilience

- 60 **Revolutionizing MTS Recovery**
by LTJG Bradley Bergan
- 63 **Trade Recovery Protocols**
by Mr. Ryan Owens
- 67 **Protecting the Supply Chain**
by CDR Carlos Torres
- 69 **Trade Recovery**
by Ms. Louritha Green

MTS Resilience

Lessons Learned from USCG Casualty Investigations

- 74 **Night Shift**
A broken autopilot and sudden loss of stability leave a fishing vessel's crew fatally shorthanded.
by Ms. Carolyn Steele
- 78 **Lethal Lifesaver**
Carbon dioxide saves a ship but claims two lives.
by Ms. Carolyn Steele

Lessons
Learned

On Deck

- | | | | |
|----|---|----|--|
| 4 | Assistant Commandant's Perspective
<i>by RADM James A. Watson</i> | 86 | Chemical of the Quarter
Understanding Methyl Ethyl Ketone
<i>by LT Sean Peterson</i> |
| 5 | Champion's Point of View
<i>by CAPT Paul Thomas</i> | | Nautical Queries |
| 91 | Upcoming in Proceedings | 87 | Engineering |
| | | 89 | Deck |

ADM Robert J. Papp Jr.
Commandant
U.S. Coast Guard

**The Marine Safety
& Security Council
of the
United States Coast Guard**

RDML Frederick J. Kenney
Judge Advocate General
Chairman

RADM Paul Zukunft
Assistant Commandant
for Marine Safety, Security
and Stewardship
Member

Mr. Jeff Lantz
Director of Commercial
Regulations and Standards
Member

RDML Cari B. Thomas
Director of Response Policy
Member

RADM James Watson
Director of Prevention Policy
Member

Mr. Dana A. Goward
Director of Marine Transportation
Systems Management
Member

Mr. Craig Bennett
Director of National Pollution
Funds Center
Member

RDML Stephen Metruck
Assistant Commandant for
Resources, Chief Financial Officer
Member

RDML Karl Schultz
Director for Governmental
and Public Affairs
Member

LCDR Erin Ledford
Executive Secretary

Ms. Kathryn Sinniger
Legal Advisor

**View PROCEEDINGS online at
www.uscg.mil/proceedings**



by RADM JAMES A. WATSON
*Director of Prevention Policy
U.S. Coast Guard*

Assistant Commandant's Perspective

We are pleased to present the winter edition of *Proceedings*, to further the ongoing discussion around securing the global supply chain—the highly complex system of infrastructure, technology, information, organizations, and people that converts raw materials to finished products and moves products and services from supplier to customer. It is the engine of our global economy, and it has to be hyper-efficient and ultra-reliable to support just-in-time delivery and uninterrupted flow of critical cargo.

Securing the global supply chain in light of this complexity, criticality, and need for efficiency, is a formidable challenge made even more daunting, as the global supply chain is owned primarily by the private sector and is regulated by international, national, state, local, and tribal entities. To help meet this challenge, the Department of Homeland Security promulgated the Strategy to Enhance International Supply Chain Security that builds on other national strategies to provide a framework for the secure flow of cargo.

The strategy has three primary goals:

- enhance the safety and security of the international cargo supply chain;
- facilitate global commerce within the enhanced security framework;
- provide for the rapid resumption of trade following an incident that disrupts the supply chain.

The Coast Guard is working with key partners to implement the strategy for the global maritime supply chain. We are focused on layered security based on sound risk assessment and ensuring rapid restoration and resumption of maritime trade if a disruption does occur. We also recognize that successful execution of the strategy will require cooperation and coordination across the wide spectrum of maritime stakeholders, particularly private sector shippers, ship owners and operators, and terminal owners and operators.

Ultimately, security must be embedded in the business practices and products of the private sector to secure the supply chain and keep it agile, efficient, and effective. We will continue to work with all maritime stakeholders, through international organizations such as the International Maritime Organization and the World Customs Organization, to achieve this end.

I look forward to your feedback on this issue of *Proceedings* and on initiatives we can jointly take to ensure a safe, secure, and efficient global maritime supply chain.

Champion's Point of View



by CAPT PAUL THOMAS
*Deputy Director of Prevention Policy
U.S. Coast Guard*

Today's global supply chain is a complex system that provides fast, efficient transport of goods and services from supplier to customer, and allows easy entrance and exit at each step as raw materials are transformed into finished products. It is open, agile, responsive, and ubiquitous. It is also potentially vulnerable to an attack or exploitation, and vulnerability in any part of the chain can have significant impact up- and downstream.

In the maritime domain, the global supply chain may be exploited to import weapons of mass destruction, be attacked to disrupt commerce, or it may be co-opted and used as a weapon (a vessel itself may be used to attack a populated area). The physical, social, and economic effects of any successful attack on or exploitation of the supply chain could be severe, long-lasting, and truly global. For the supply chain to be effective, efficient, and reliable, it must be secure.

The articles in this issue describe the global system to ensure supply chain security through awareness, protection and prevention measures, response, and recovery. Taken together, these basic elements provide the framework for risk-based, layered security that balances threat mitigation with the need for an effective, open supply chain.

Awareness is essentially a function of how well information is collected and shared, and several of the articles describe efforts to improve information sharing as a means to enhance security, safety, and efficiency. Several of the articles relate to ongoing international coordination necessary to secure the supply chain that crosses every jurisdictional boundary in the world. Active engagement and participation of public and private sector stakeholders is absolutely essential to the successful implementation of protection and prevention regimes. Several articles address the public/private partnerships that are designed to enhance supply chain security while reducing the burden of the security measures themselves.

Finally, when a disruption to the global supply chain does occur, rapid response and recovery is essential—not only to resume trade, but to aid the larger recovery effort. A number of articles address marine transportation system recovery, recognizing that many different types of incidents can occur—both natural and man-made. System resiliency requires planning for and responding to all threats and all hazards.

The degree of interconnectivity and interdependency among nations, organizations, businesses, and people within the global supply chain will continue to increase as the volume of worldwide trade, particularly maritime trade, increases in the coming decades. Our imperative as a maritime community is clear: We must continue to seek innovative, cooperative, and sustainable measures to enhance global supply chain security. We hope this issue of *Proceedings* will advance that effort.

Editorial Team

Barbara Chiarizia
Executive Editor

Leslie C. Goodwin
Art Director

Sarah K. Webster
Managing Editor

Proceedings is published quarterly by the Coast Guard's Prevention Directorate, in the interest of safety at sea under the auspices of the Marine Safety & Security Council. Special permission for republication, either in whole or in part, except for copyrighted material, is not required, provided credit is given to *Proceedings*.

The articles contained in *Proceedings* are submitted by diverse public and private interests in the maritime community as a means to promote maritime safety and security. The views expressed by the authors do not necessarily represent those of the U.S. Coast Guard or the Department of Homeland Security or represent official policy.

Editorial Contact

HQS-DG-NMCPProceedings@uscg.mil

Editor, *Proceedings* Magazine
U.S. Coast Guard
2100 2nd Street SW Stop 7681
Washington, D.C. 20593-7681

www.uscg.mil/proceedings

202-372-2316

Subscription Requests/Changes

Proceedings is free.

Please include mailing label information when changing address.

Subscriptions, *Proceedings* Magazine
U.S. Coast Guard
Attn: *Proceedings* Magazine
2100 2nd Street SW Stop 7681
Washington, D.C. 20593-7681
www.uscg.mil/proceedings



The Secure Chain

Interactions among supply chain members can ensure security.

by MR. ANTHONY BARONE
*Director, Global Logistics Policy
Pfizer Global Manufacturing*

There are many threats involved in the global waterborne shipment of goods. Corporations and government entities face the possibility that something or someone is out there looking to compromise their shipping operation. Risks include smuggling, pilferage, or damage. Other times, the culprit is not a person, group, organization, or entity, but rather nature herself; heavy winds and storms can cause significant cargo contamination, spoilage, and other damage.

Shipping companies, as well as the countries from which and to which goods are shipped, all shared these concerns prior to the 9/11 terrorist attacks on the United States. Transnational threats are not something new, but today they come with new concerns about security threats, such as a conveyance being used without the knowledge of the cargo owner or carrier to deliver a weapon of mass destruction or to further terrorist activity in some way.

These are some examples of reasons why it is important to have a secure supply chain program that begins well before cargo is loaded aboard a vessel. Therefore, it is imperative to focus on supply chain security from the private sector and governmental points of view, as the two are intimately related.

The First Links in the Chain

A typical manufacturing process starts with raw material moving from several places to a facility where it is converted into a semi-finished good. The work-in-process may then move to other locations where further processing takes place until the finished consumer good is produced.

All the risks mentioned above are operative at each step in the process. In the case of a food or medi-

cine—especially those that require transport within a narrow temperature/humidity range—constant monitoring is needed to assure quality and safety.

If a loss occurs in any part of the supply chain, the impact can be felt all the way to the finished product and its customer. In industries that rely on just-in-time manufacturing techniques, any delay in any part of this complex system can cause disruptions that are felt worldwide. For example, in single-source manufacturing environments, interruptions may affect every customer around the world receiving goods from the factory that experienced the interruption.

The Relationships Among the Economic Operators

It's important to emphasize that cargo safety and security is not the exclusive domain of government. Protecting against theft, damage, contraband, dangerous cargo spills, counterfeit inclusion, and introduction of articles intended to hurt or kill, are also the concern of shippers of cargo and the carriers that provide transportation and distribution services. As with any business function, the intensity and effectiveness of supply chain integrity programs can vary.

For example, shippers of valuable or "pilferable" goods, such as pharmaceuticals, consumer electronics, and cosmetics often hire armed escorts and/or practice other heightened security measures to assure the integrity of their supply chains. Those that ship less valuable commodities may not be able to afford the same level of protection, nor does that cargo typically require it. This creates a continuum of risk that government and trade must consider with regard to protective measures.

continued on page 8

Glossary of Shipping Terms

When looking at the supply chain, it helps to understand some of the key words and phrases used in the transportation industry.

Agent: A person authorized to transact business for and in the name of another person or company. Types of agents include: brokers, commission merchants, resident buyers, sales agents, manufacturer's representatives.

Aggregate Shipment: Numerous shipments from different shippers to one consignee that are consolidated and treated as a single consignment.

All In: The total price to move cargo from origin to destination, inclusive of all charges.

ATDNSHINC: Any Time Day or Night Sundays & Holidays Included. This is a chartering term that refers to when a vessel will work.

Bill of Lading: A document that establishes the terms of a contract between a shipper and a transportation company. It serves as a document of title, a contract of carriage, and a receipt for goods.

Break Bulk: (1) To unload and distribute a portion or all of the contents of a rail car, container, trailer, or ship. (2) Loose, non-containerized mark and count cargo. (3) Packaged cargo that is not containerized.

Broker: A person who arranges for transportation of loads for a percentage of the revenue from the load.

Bulk Cargo: Not in packages or containers; shipped loose in the hold of a ship without mark and count. Grain and coal are usually bulk freight.

Carrier: Any person or entity who, in a contract of carriage, undertakes to perform or to procure the performance of carriage by rail, road, sea, air, inland waterway, or by a combination of such modes.

Certificate of Origin: A certified document showing the origin of goods, used in international commerce.

Charter Party: A written contract between the owner of a vessel and the person desiring to employ the vessel (charterer). Sets forth the terms of the arrangement, such as duration of agreement, freight rate, and ports involved in the trip.

COGSA: Carriage of Goods by Sea Act. U.S. federal codification passed in 1936 that standardizes carrier's liability under carrier's bill of lading and the U.S. enactment of The Hague Rules.

Common Carrier: A transportation company that provides service to the general public at published rates.

Conference: An association of ship owners operating in the same trade route who operate under collective conditions and agree on tariff rates.

Consignee: A person or company to whom commodities are shipped.

Consignee Mark: A symbol placed on packages for identification purposes, generally a triangle, square, circle, etc. with letters and/or numbers and port of discharge.

Consignor: A person or company shown on the bill of lading as the shipper.

Container: A truck trailer body that can be detached from the chassis for loading into a vessel, a rail car, or stacked in a container depot. Containers may be ventilated, insulated, refrigerated, flat rack, vehicle rack, open top, bulk liquid, or equipped with interior devices. A container may be 20, 40, 45, 48 or 53 feet in length, eight feet or eight feet, six inches in width, and eight feet, six inches or nine feet, six inches in height.

Container Load: A load sufficient in size to fill a container either by cubic measurement or by weight.

Customhouse Broker: A person or firm, licensed by the treasury department of their country when required, engaged in entering and clearing goods through customs for a client (importer).

Deadweight Cargo: A long ton of cargo that can be stowed in less than 40 cubic feet.

Demurrage: A penalty charge against shippers or consignees for delaying the carrier's equipment or vessel beyond the allowed free time. The free time and demurrage charges are set forth in the charter party or freight tariff.

Drayage: Charge made for local hauling by dray or truck. Same as cartage.

Freight: Refers to either the cargo carried or the charges assessed for carriage of the cargo.

Freight Bill: A document issued by the carrier based on the bill of lading and other information, used to account for a shipment operationally, statistically, and financially.

Freight Forwarder: A person whose business is to act as an agent on behalf of the shipper. A freight forwarder frequently makes the booking reservation. In the United States, freight forwarders are licensed as "ocean intermediaries."

Hague Rules, The: A multilateral maritime treaty adopted in 1921 (at The Hague, Netherlands), standardizes liability of an international carrier under the Ocean Bill of Lading.

Landbridge: Movement of cargo by water from one country through the port of another country, thence using rail or truck, to an inland point in that country or to a third country.

LCL: Abbreviation for "Less than Container Load." The quantity of freight that is less than that required for the application of a container load rate. Also known as "loose freight."

Liner: A vessel advertising sailings on a specified trade route on a regular basis. It is not necessary that every named port be called on every voyage.

Mixed Container Load: A container load of different articles in a single consignment.

Non-Vessel Operating Common Carrier (NVOCC): A cargo consolidator in ocean trades who will buy space from a carrier and sub-sell it to smaller shippers. The NVOCC issues bills of lading, publishes tariffs, and otherwise conducts itself as an ocean common carrier, except that it will not provide the actual ocean or intermodal service.

Ocean Bill of Lading: A contract for transportation between a shipper and a carrier. It also evidences receipt of the cargo by the carrier. A bill of lading shows ownership of the cargo and, if made negotiable, can be bought, sold, or traded while the goods are in transit.

Shipper: The person or company who is usually the supplier or owner of commodities shipped; also called consignor.

SSHEx: Abbreviation for Saturdays, Sundays, and Holidays Excepted. Refers to loading and discharging of cargo as agreed to in the charter party. This indicates when time does not count in the calculation of demurrage and despatch.

Waybill: A document prepared by a transportation line at the point of a shipment: shows the point of the origin, destination, route, consignor, consignee, description of shipment, and amount charged for the transportation service. It is forwarded with the shipment or sent by mail to the agent at the transfer point or waybill destination. Abbreviation is WB. Unlike a bill of lading, a waybill is not a document of title.

Windy Booking: A freight booking made by a shipper or freight forwarder to reserve space but not actually having a specific cargo at the time the booking is made. Carriers often overbook a vessel by 10 to 20 percent in recognition that "windy booking" cargo will not actually ship.

"Glossary of Shipping Terms." United States Maritime Administration, 2008.



The Human Element

When looking at the human element within a supply chain, the following example illustrates the concerns.

The supply chain starts at a factory, where a palletized shipment of talc is loaded on a less-than-load motor carrier that delivers the cargo to a pool consolidator.

The consolidator (also known as non-vessel operating common carrier) holds the pallet in the warehouse as freight accumulates.

At the end of the week, when enough freight has been accumulated, a 20-foot container is loaded and shipped by ferry.

The container is then drayed by another motor carrier to the port where the box is received into a marine terminal.

A drayman inside the terminal then moves the box to the vessel on which it is loaded.

Before loading onto a vessel, the fictitious pallet changed hands many times.

To a significant degree, risk is related to the frequency of exposures to threats, so every time the pallet changed hands, it was exposed to a threat.

Additionally, operating in high-crime regions can raise the theft risk profile. But high crime, such as narcotics trafficking, might not raise the terrorism risk. What is common to these scenarios is the relationship that exists among the trading parties or “economic operators.”

From the logistician’s point of view, security is a multi-faceted issue. Conveyance security is about protecting the cargo from all likely dangers including terrorism. To that end, some basic strategies predominate.

For example:

Eliminate dwell time. Cargo at rest is cargo exposed.

Ensure container integrity. Employing security seals on drums and on freight containers is not entirely reliable. Containers must be thoroughly inspected before loading and when they arrive at a destination for unloading. Additionally, sophisticated electronic container devices can monitor interior conditions and position.

Don’t ignore the human element. Shippers must know who they are engaging to move cargo.

Partnerships

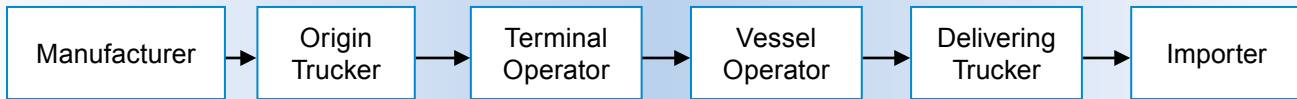
Assuring security in the supply chain is a function of the effectiveness of managing risks in these relationships. In the United States, companies that have instituted strong security programs are admitted into a special customs program known as the Customs-Trade Partnership Against Terrorism, or C-TPAT. It’s a voluntary program led by U.S. Customs and Border Protection (CBP) that seeks a partnership with the trade to prevent the possibility that freight conveyances entering the United States may be used to deliver a weapon of mass destruction. Today, there are more than 10,000 certified member companies participating in the C-TPAT program.

On a global basis, these companies that are willing to demonstrate strong security profiles are granted certain privileges. The most relevant of these is fewer cargo inspections. Fewer cargo inspections mean fewer supply chain interruptions and more predictable supply.

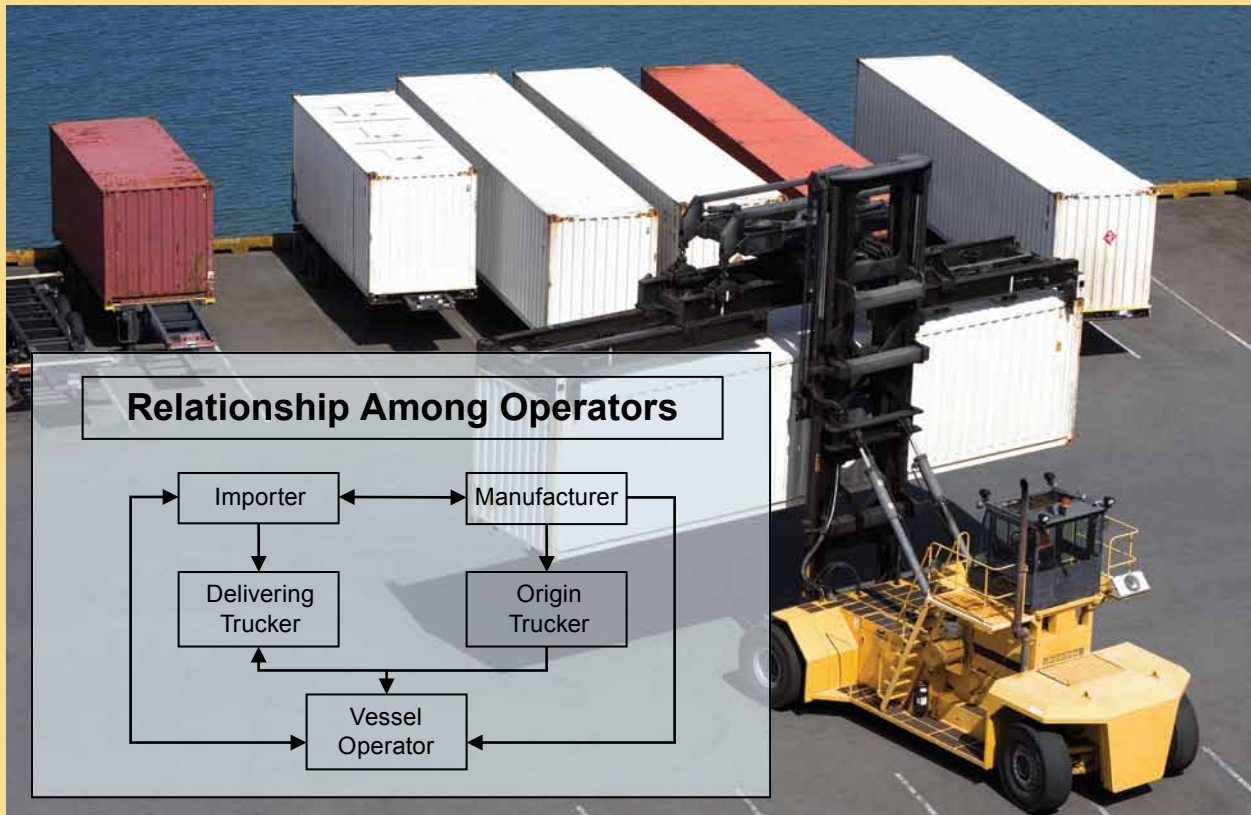
Theoretically, those are good enough reasons to implement strong security programs. But the statistical probability of such inspections is relatively low,

continued on page 10

Supply Chain Economic Operators



The relationships in a simple supply chain. The manufacturer engages the trucker, who carries freight to a terminal, who loads the vessel. Eventually, the cargo reaches the importer.



In terms of determining risk, all parties involved will have many questions. For example:

- Is the manufacturer reliable?
- Does the company have a track record?
- What do other customers say about the manufacturer?
- Does it have strong quality controls?
- Is the country of manufacture safe from the shipping point of view?
- Is there adequate transportation service or is the freight going to be exposed to dwelling risk?
- Is there a risk of conveyance infiltration?

The relationship and selection of carrier from the manufacturer to the port is typically left to the manufacturer because the importer often is in another country. Minimizing risk of transportation at origin is the domain of the supplier, which can engender more questions.

- Does the trucker employ reliable drivers?
- Are there background checks as permitted by law?
- Is the equipment secure?
- Are the trucker's yards secured?

- Is there tracking equipment?
- Do other customers have a positive relationship?
- Is the company financially stable?
- Does it have a history?

Facility personnel on both ends and carriers (if there is an equipment interchange) will want to know who to allow in the facility. The vessel operator will want to know about the shipper as well as terminal operators at both ends.

in any country, depending on the risk profile of the origin country. Other compelling reasons to secure supply chains are the commercial reasons cited. Companies that recognize and invest in supply chain security for commercial reasons are recommended to take advantage of these customs benefits. Sometimes, that means a relatively modest incremental investment.

The SAFE Framework (Framework of Standards to Secure and Facilitate Global Trade), an international convention to which most of the world's countries belong, recognizes the idea of economic operators (supply chain partners) and the concept that certified operators are less risky and deserve fewer inspections and "simplified" importation processes. These companies are referred to as authorized economic operators or AEOs.

The Bottom Line

A fundamental feature of these programs: Importers seek to assure that foreign suppliers adhere to the security principles laid out in the program. Certified members should have strong security programs and be willing to leverage their business relationships to ensure that suppliers and logistics services providers implement equally effective security programs.

This can run contrary to a basic principle of business—buying from the lowest-cost supplier. What if the supplier rejects the required security measures and the only alternative supplier costs more? Fidelity to security principles is made easier when ancillary commercial considerations serve to underwrite the costs and efforts needed to assure compliance. Management willingness to invest money into the program is facilitated by fewer inspections as well as the broader benefits of enhanced security.

Another fundamental feature of these partnerships is that the trader understands its supply chain and the inherent risks within it. An assessment of the chain will yield a focused assessment of the trader's vulnerability and from that should come a gap analysis and plan on how to enhance security. The trader should ask questions like:

- Who participates in the supply chain?
- Where are they?
- What are the known risks in that part of the world?

- Are the risks high or low?
- What is the current risk level associated with that transportation lane?
- How secure are the operators in the supply chain?

These kinds of inquiries require constant vigilance. Yesterday's information may not be good for today, and keeping up with the latest intelligence can present a challenge. Additionally, companies with thousands of supply chains have bigger challenges than smaller companies that deal with one or two foreign suppliers.

Most of this discussion has been from the point of view of the trader in goods: manufacturers, exporters, and importers. Carriers, on the other hand, face a different but analogous problem when a sealed container is loaded on a container ship or a netted pallet is loaded aboard an airplane. Neither party can see the contents in the container. Therefore, the relationship among the parties becomes an important part of the overall security environment. If each supply chain partner (including the supplier, the trucker, the carrier, etc.) is safe and secure, then the supply chain is safer than if any link is not known or not known to be safe. C-TPAT addresses this by certifying each supply chain member separately. If the importer, vessel operator, forwarder, broker, drayman are certified members, vulnerability is reduced.

In a perfect world, C-TPAT and other AEOs would form an impregnable network that terrorists and organized crime could not penetrate. Unfortunately, none of us live in a perfect world. Still, the precepts of AEO and C-TPAT—know your suppliers, know your customers, stay vigilant, engage senior management, understand your threats, and understand your vulnerabilities—are all good defensive layers that can make the job of an intruder that much more difficult.

About the author:

Mr. Anthony Barone is the director of Global Logistics Policy at Pfizer Global Manufacturing. He served on the customs operations advisory committee of the U.S. Department of Homeland Security from 2005 to 2009. He has also served as a consultant in international logistics and trade finance in 2001, held senior positions in the third party logistics industry and with supply chain IT developers, and provided in-country consulting to the Agency for International Development and to FEMA. He is a graduate of Columbia University and holds an MBA.

The Coast Guard and Customs and Border Protection Partnership

Securing an evolving maritime supply chain.

by LCDR DAN SOMMA
U.S. Coast Guard
Branch Chief, Cargo and Facility Security

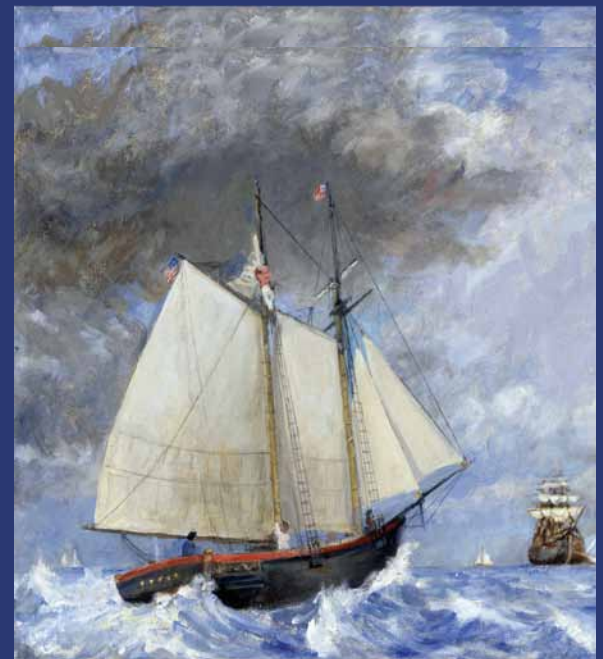
Ms. JEN CLIMENHAGA
U.S. Customs and Border Protection

Cash-strapped after the revolution, the new government established the U.S. Customs Service in 1789. Because post-Revolutionary War smuggling was still alive and well, Secretary of the Treasury Alexander Hamilton championed the construction of 10 revenue cutters in 1790.

This Revenue Cutter Service was the predecessor to the modern U.S. Coast Guard, and while customs operations now fall under the umbrella of U.S. Customs and Border Protection (CBP), the relationship established to protect the nation more than 200 years ago continues.



Inspection of a Merchant Ship by Gil Cohen



Grandfather of the Coast Guard by Agnes Davis

Throughout the era of sailing ships, the two agencies under the Department of Treasury enjoyed a strong working relationship with dedicated mission areas in the supply chain. The U.S. Coast Guard inspected ships for compliance with federal laws while U.S. Customs and Border Protection did the same for the cargo. As the industry grew and evolved, both agencies had to work harder and become smarter.

Containerization

At the end of World War II, idle U.S. vessel tonnage would be put to use in creative ways, and would generate business opportunities not foreseen in the Revenue Cutter days. A particularly important challenge was the birth of containerization, which greatly sped up the world's supply chains.

Malcolm McClean was no expert in ships, but managed to change the shipping industry forever. As co-owner of McLean Trucking Company he realized the transition from one mode (sea) to another (land) took too much time and ate into profits. Ships were tied up to the dock too long while gangs of longshoremen loaded or unloaded the cargo.

To speed this process, the American entrepreneur proposed placing the cargo in containers in the first place. This way a truckload of cargo could be transferred from one mode to another with minimal delay. In 1956, this vision was realized with the shipment of 58 boxes on the deck of a tank ship. By 1960, with several WWII-era vessels in service, the world's first intermodal maritime container service was born.

The Impact on Security

It was no surprise that containerization presented some unique challenges for cargo inspection. First, because of the speed at which a container vessel could be offloaded, mandated inspections on the vessel could no longer be done on the government's schedule, they had to be done much more quickly to meet tight turnaround times.

Container ships also traveled faster, easily exceeding 22 knots, and stayed at the dock for far less time than a comparable break bulk carrier. Each ship contained hundreds (and eventually thousands) of containers, each container with an individual manifest of contents. To increase the complexity, the vessel and terminal operators typically took the manifest at face value, as they did not have the time to verify everything in the document. Terminals and ship design evolved to keep cargo on the move, since cargo on the move makes money.

But, the inherent movement of cargo ultimately improved security, since it is harder to pilfer, tamper with, or steal cargo that is on the move. Lost and pilfered cargo, accepted as a cost of doing business in days past when cargo waited days and weeks to make it onto a ship, became less tolerated. Ships with tight turnarounds offered less opportunity for smugglers or stowaways.

What This Means Today

Inspection and enforcement authorities, too, were forced to adapt to the increasing speed of the system. By the late 1980s, industry grew to rely on "just-in-time" shipping for many goods, so instead of storing a warehouse full of clothes, a retailer relied on container loads already in the supply chain. For example, a load of blue jeans going to a U.S. retailer from a factory in China, via Shanghai to Long Beach, Calif., is constantly in motion. Using enabling authorities from the Maritime Transportation Security Act of 2002 and the Security and Accountability of Every Port Act of 2006, the Coast Guard and CBP have introduced new layers of security around that shipment to ensure that the blue jeans really are what they say they are on the manifest.

Manifest information for cargo being shipped by sea (in this case of our blue jean shipment, via container vessel) must be submitted to Customs and Border Protection at least 24 hours before the container is loaded onto a ship headed to the United States. The "24-hour rule" has given CBP a greater window of time to do vital screening and targeting work.

Since 2009, additional information is required under the Importer Security Filing and Additional Carrier Requirements or "10+2." The 10+2 requirements mean that importers and carriers must submit additional information pertaining to cargo to CBP before the cargo is brought into the United States by vessel. The 10 additional elements from the importer (including seller, buyer, and country of origin) and two from the carrier (container stuffing location and consolidator), give CBP a more robust picture of "what's in the box."

The Container Security Initiative

Customs and Border Protection designates Container Security Initiative (CSI) officers who work with host foreign government counterparts to conduct manifest reviews and target high-risk cargo.

Pre-screening and evaluating containers as early in the supply chain as possible helps facilitate the movement of legitimate trade. Ideally, this is done before

shipment, generally at the port of departure. CBP officers review manifests for containerized cargo destined for the United States and target cargo that poses a risk for terrorism. Then stateside Customs and Border Protection officers use non-intrusive inspection equipment, including large-scale x-ray and gamma-ray imaging systems and radiation detection equipment, to inspect high-risk cargo at the first port of arrival into the United States.

Container Security Initiative is now operational at ports in North America, Europe, Asia, Africa, the Middle East, Latin, and Central America. CSI prescreens more than 80 percent of all maritime containerized cargo imported into the United States.

eNOAD, C-TPAT

Additionally, the Coast Guard and CBP coordinated and developed an online electronic arrival and departure manifest system for the requirements of both agencies. As such, 96 hours prior to arrival, a U.S.-bound vessel must submit an electronic notice of arrival/departure (eNOAD) to the U.S. Coast Guard National Vessel Movement Center. An eNOAD manages and stores company, vessel, personnel, and arrival information and can be submitted directly to the National Vessel Movement Center even while the vessel is underway. Additionally, it contains a general description of the cargo and crew details, giving CBP and Coast Guard officers enhanced maritime domain awareness.

Another layer in the security of the supply chain is the voluntary Customs-Trade Partnership Against Terrorism or C-TPAT, which is a cooperative program for partners in supply chain security, including importers, carriers, consolidators, licensed customs brokers, and manufacturers. Through C-TPAT, businesses ensure the integrity of their security practices and verify the security guidelines of their business partners within the supply chain. Some industry benefits of C-TPAT membership include reduced number of CBP inspections (reduced border delay times) and priority processing for CBP inspections.

How This Works Aboard the Vessel

Going back to the example of our blue jean shipment, after proper notification by the shipper and after proper screening by the CSI port in Asia, the cargo is loaded using a computer-aided planning system and robotic cranes. The position of each container is segregated for safety by requirements

set in the International Maritime Dangerous Goods code, which ensures the safest position for each load.

The vessel crew is trained to internationally approved standards and has been carefully screened by the ship operator. As they cross the Pacific Ocean, the vessel participates in long range information and tracking and broadcasts its position by radar signature and the Automated Information System (AIS).

The ship also employs a ship security alert system, under which all of the security onboard is the responsibility of the ship security officer (often the captain or the first mate) who relays any security concerns to a company security officer. As they approach Long Beach, the crew makes contact over radio and by AIS to the Coast Guard and pilots who bring them into dock.

The Coast Guard captain of the port has jurisdiction for the vessel entry into the port while the CBP port director will have authority over the cargo and the crew once they arrive. The captain of the port uses a baseline risk assessment for the port developed using the Maritime Security Risk Assessment Model. This model gives a comprehensive risk picture of threats, likelihood, and consequence of a range of scenarios.

Meanwhile, the Customs and Border Protection port director has information from the CBP's National Targeting Center for Cargo and National Targeting



Coast Guard Petty Officer Chelsea Warren and Customs and Border Protection Officer Michael Henderson verify a Transportation Worker Identification Card. U.S. Coast Guard photo by Petty Officer Robert Brazzell.



Members of the Coast Guard and Customs and Border Protection inspect a vessel during a joint boarding. U.S. Coast Guard photo by Petty Officer Bobby Nash.

Center for Passengers to help guide decisions on who and what to inspect upon arrival.

Security is coordinated locally by the Port of Long Beach Command and Control Center, in which several agencies with security responsibilities like the Coast Guard and CBP are co-located under the same roof. (Other examples are the Joint Maritime Advanced Scheduling and Targeting Team, Jacksonville; the Seattle Joint Harbor Operations Center; and the Charleston Joint Harbor Operations Center).

From such a center, CBP and the Coast Guard can target vessel, crew, and cargo for inspection upon arrival. A boarding at sea may be coordinated if the risk is determined to be high enough. It is the job of the Coast Guard port state control inspectors to inspect all aspects of foreign ships for safety provisions including compliance with the International Ship and Port Facility Security Code. Often Coast Guard and CBP are on the vessel at the same time checking mariner documents (CBP for admissibility requirements and Coast Guard for crew competency). Ships deficient in any area can receive a captain of the port order, "form B" deficiency, or SOLAS detention, or customs hold.

The containers aboard the ship are declared upon entry. Coast Guard container inspectors will target

shipments for hazardous materials and Coast Guard facility inspectors will verify provisions of the facility security plan are in place. Using handheld readers, the Coast Guard can verify the authenticity of Transportation Worker Identification Credentials.

Containers chosen by CBP, or by Coast Guard request, will pass through the vehicle and cargo inspection system, which conducts a non-intrusive scan of the container contents. Sometimes the container will be opened for inspection, other times it will not. All containers are screened for radiological signature prior to leaving the port area. Then the blue jeans will continue their journey to a store, either by truck or by rail.

Looking Ahead

Much of the above regime is the result of enhancement after the 9/11 terrorist

attacks. And while there were up-front challenges, the industry, in an effort to make sure cargo could continue to flow freely and securely, made the necessary modifications to its operations to make sure CBP's data needs were met. As is usual for new CBP rules and regulations, extensive outreach to the trade was conducted to ensure a wide dissemination of information.

CBP's Office of Trade holds seminars and outreach events, posts information widely on the Internet, and makes top officials available routinely to the trade through regular meetings of the Commercial Operators' Advisory Committee and the Customs Electronic Systems Advisory Council.

The Coast Guard maintains many mechanisms for security outreach, primarily using area maritime security committees as disseminating points for vital security information. The National Maritime Security Advisory Committee is an industry sounding board for new ideas and updates on proposed regulations. Nationally, the Coast Guard hosts a national Harbor Safety Conference and Area Maritime Security Committee meeting during which maritime security topics are discussed openly with the public.

At the highest levels, the Coast Guard and Customs and Border Protection coordinate operations, out-

reach, and training through the Senior Guidance Team. Chaired by the Commissioner of CBP and the Commandant of the Coast Guard, this team ensures that the two agencies are doing everything they can to share information, improve interoperability, and raise the level of security at the border and beyond.

While supply chain security has become more complicated, more active, and more global, by relying on an historical partnership and a suite of new regulations, procedures, and technologies, CBP and the Coast Guard have been able to meet the challenges of a secure, modern, global supply chain.

About the authors:

LCDR Somma is the branch chief of cargo and facility security at Coast Guard headquarters. He previously served as a container, facility, and vessel inspector in the ports of Seattle/Tacoma and New

York/New Jersey. He holds an MS in transportation management and is a recipient of the U.S. Customs' Best Practice Award for Joint Targeting and Inspection.

Officer Jen Climenhaga has held a variety of positions within U.S. Customs Border Protection, including assignments in the Office of Field Operations, the Office of International Affairs, and a detail to the Office of Public Affairs. She is currently on temporary detail as a CBP liaison to the Department of Homeland Security Domestic Nuclear Detection Office. Prior to the creation of DHS, Officer Climenhaga was an inspector with the U.S. Customs Service.

Bibliography

- Chernow, Ron, "Alexander Hamilton," pg. 290, 2004.
- Fretelli, John, <http://www.fas.org/sgp/crs/homsec/RL31733.pdf>
- Haddal, Chad, "Border Security: Key Agencies and their Missions," Congressional Research Service Report, January 26, 2010. <http://www.fas.org/sgp/crs/homsec/RS21899.pdf>
- Levinson, Marc, "The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger," Princeton University Press, Princeton, NJ, 2006.
- Walsh, Don, "Box Boats—Delivering the World's Stuff," U.S. Naval Institute Proceedings, May 2011.



The National Strategy for Global Supply Chain Security

The path to an intermodal security program.

by Ms. MARANDA SORRELLS
Policy Advisor
U.S. Department of Homeland Security

MR. MICHAEL CALLAHAN
Program Analyst
U.S. Coast Guard Office of Emerging Policy

MR. SEAN MOON
Senior Policy Advisor
U.S. Department of Homeland Security

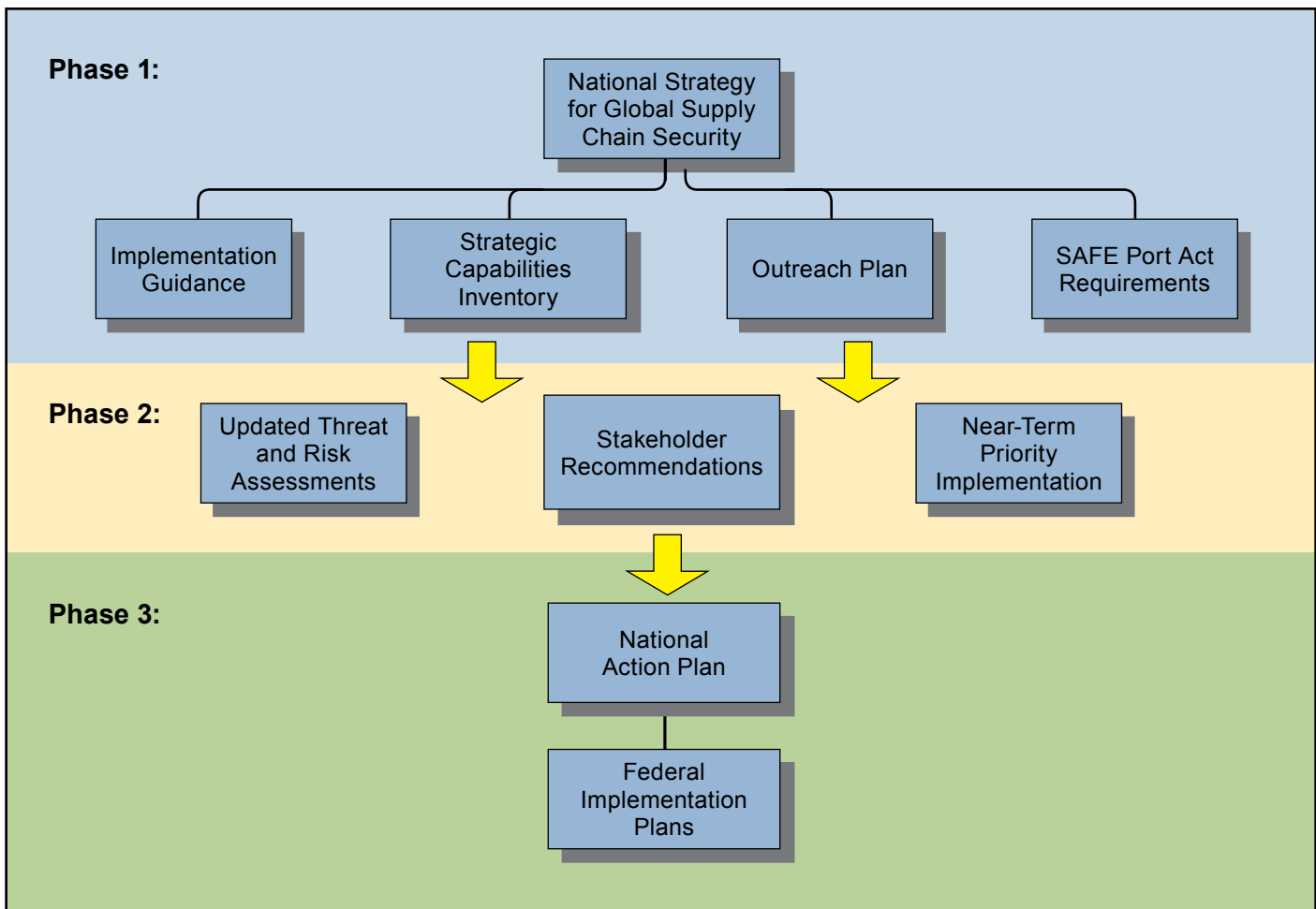
Setting the Scene

In any factory in any country, goods are created to satisfy consumer demand. For our purposes, let's assume that commodity X is in high demand in the United States. Big box stores place an order for commodity X, and a factory in a foreign country produces it.

Fulfillment personnel ship commodity X to the port in trucks. From there the shipment is consolidated and loaded onto a ship. The ship then sails to the United States, where the cargo is off-loaded to trucks or rail cars and transported to a warehouse or distribution center. From the distribution center, the goods from the cargo are loaded onto trucks and delivered to the big box store.

This generally describes the global supply chain and illustrates myriad avenues for disruption to which it is susceptible. For example, the fulfillment factory may be damaged by an earthquake, shut down by a labor strike, or targeted as a critical commodity producer for terrorist action. Thieves may hi-jack the trucks. The port may be shut down by civil unrest. The ships may be lost at sea, captured by pirates, or worse, exploited by terrorists who are intent on doing harm to the United States or its trade partners.





The National Strategy for Global Supply Chain Security will be implemented in three main phases, starting with initial release in late 2011, continuing through immediate actions, outreach, data gathering, culminating in a national action plan, and federal implementation plans.

The U.S. National Strategy to Secure the Global Supply Chain represents our best effort to pave a path forward toward a secure system that maintains the free and efficient flow of goods from point of origin to point of sale through any disruption.

Overview

Two overarching goals guide the U.S. government’s global supply chain efforts:

- “secure efficiency” to enhance the security and efficiency of the global supply chain,
- “dynamic resilience” to strengthen the resilience of the global supply chain against catastrophic disruptions.

At its core, the strategy is about managing risks through a layered approach that capitalizes on focused measures aimed at increasing security and resilience, and improving functionality and efficiency.

Specifically, the strategy recognizes the need for the U.S. to work in concert with other nations and private sector partners to:

- ✓ implement security measures throughout the global system by deterring terrorists or other bad actors from exploiting it as a channel for delivering harm,
- ✓ protect infrastructure critical to the continued operation of the system,
- ✓ embed resilience throughout the system.

The strategy also recognizes that the United States must work to improve its domestic system for moving commerce. To improve system efficiency and functionality, the strategy must first streamline and reform government security processes.

This means the U.S. government will work to remove unnecessary security-related obstacles from the flow

The Strategy

The National Strategy to Secure the Global Supply Chain began as a Department of Homeland Security (DHS) effort to fulfill a congressional requirement of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act).

In keeping with the focus of the act, an initial DHS strategy created in 2007 was predominantly maritime-centric. After discussion, however, the National Security Staff (NSS), in concert with DHS, felt that a whole-of-government harmonized approach was needed to foster more informed resourcing and lay the groundwork for broad international collaboration.

So DHS, the NSS, other government agencies, and a broad spectrum of supply chain stakeholders developed the new strategy by building upon the National Security Strategy, the National Strategy for Aviation Security, the Surface Transportation Security Priority Assessment, the National Strategy for Maritime Security, and its supporting plans and other existing strategies and guidance.

The new strategy expands its scope beyond the SAFE Port Act requirements by addressing all cargo modalities (air, land, and sea) and by seeking to improve the security of the goods, conveyances, and infrastructure that make up the system, as well as the people responsible for efficiently and effectively moving lawful commerce.

For the purposes of the national strategy, the global supply chain encompasses the entire worldwide

network of transportation assets and infrastructure by which raw materials or finished goods are moved between and among various points of extraction, manufacturing, assembly, and warehousing until they reach an end consumer.

From Release to Action

The strategy will be released and implemented in phases, with initial release as the first phase in the fall of 2011. It will consist of multiple interlocked documents in two sets. The first set will be the national strategy itself, and implementation guidance for short-term actions. Accompanying these documents will be a capabilities inventory in support of the National Strategy for Global Supply Chain Security, an outreach plan, and a report that addresses fulfilling SAFE Port Act requirements.

The 180-day second phase will involve realizing the administration's near-term priorities, updating and creating threat and risk assessments, and eliciting stakeholder input toward implementation.

Once the second phase information has been gathered, the interagency will develop a follow-on third effort in mid-2012 to prioritize future action and create a national action plan. From this document, departments and agencies will create their own customized implementation plans that will influence upcoming budgets and activities, fulfilling the strategy's goals and objectives by realizing the framework of the capabilities inventory.

of lawful commerce and continuously look for ways to improve, reform, and optimize security measures. The administration will also put new emphasis on adapting and developing new technologies that achieve greater security and efficient movement of commerce. Finally, the U.S. government will expand, develop, and modernize supply chain and border infrastructure by working with Canada and Mexico to assess needs and develop solutions to address them.

Implementation Guidance

A specific set of actions for the federal government accompany the strategy, outlining activities to be

undertaken in the near term to enhance supply chain security and facilitate further development and implementation phases.

The recommendations fall into four categories:

- securing and facilitating the flow of maritime containerized cargo,
- strengthening the security and facilitation of air cargo,
- securing and facilitating North American commerce,
- building resilience and expediting trade through infrastructure improvements.

Additionally, the implementation guidance provides a brief explanation of each category, current efforts focused on the problem, and next steps and actions to address it, including, in the instance of North American commerce, approaches to pursuing the strategy's objectives with our border partners Canada and Mexico.

Capabilities Framework

A key component of the strategy development effort involved an extensive analytic process to create a capabilities framework by which to define a desired end-state and measure progress toward a more secure supply chain. Led by a core team from across DHS, an interagency advisory group of subject matter experts consulted with hundreds of supply chain stakeholders, think tanks, and academia to construct an architecture of functional capabilities necessary to reach strategic policy goals. For each of the goals, the team also developed subordinate objectives and measurable tasks.

The functional capabilities outline a layered security approach that includes personnel, cargo, and infrastructure surety and verification, response actions, and systemic resilience. The team wrote the capabilities with enabling functions so that the tools needed to pursue the strategy (information management, strong domestic and international partnerships, and harmonized standards) were provided.

Goals, Objectives, Actions

By way of example, "Goal 1" in the capabilities inventory is to secure the lawful flow of goods while facilitating efficient and reliable commerce flow. Supporting this goal are three objectives, the first of which is to ensure cargo integrity and identify activities of interest.

This objective contains three actions:

- ✓ establish confidence in cargo integrity and transparency,
- ✓ identify activities of interest and verify cargo materials,
- ✓ maintain cargo integrity.

In turn, each of these actions identifies lead and supporting U.S. government members whose participation is necessary to achieve the overarching goal.



USCG photo by Petty Officer Cory J. Mendenhall

Throughout the supply chain, disruptions caused by Mother Nature or malicious people challenge efforts to maintain a free and open flow of goods.

As such, these capabilities will form the framework of the national action plan as well as federal agency implementation plans.

Outreach

The fourth document in the initial release is the outreach plan. Given that stakeholder collaboration is critical to achieving the administration's goals across the global supply chain system, the strategy includes a detailed outreach plan. To engage with private sector stakeholders, the outreach plan uses the Cross-Sector Supply Chain Working Group, under the Critical Infrastructure Partnership Advisory Council. Through this council, the government can solicit and compare ideas with the private sector without co-opting one or the other's integrity as an exclusively private or public organization.

The global supply chain system affects everyone, and implementing solutions requires your participation.

International engagement will be pursued through direct bilateral discussions with interested parties, via an Internet-based comment system, and through international organizations such as the Asia-Pacific Economic Cooperation, the International Maritime Organization, the International Civil Aviation Organization, and (predominantly) the World Customs Organization. Some engagement is already underway through a DHS initiative that seeks international collaboration on supply chain issues across the air, land, and sea modes.



SAFE Port Act Requirements

The final document in the national strategy suite specifically addresses the requirements of the SAFE Port Act that are not addressed elsewhere to directly communicate how the strategy fulfills the congressional mandate. These requirements include:

- an economic analysis of supply chain security measures and consideration of small business impacts,
- potential incentives and voluntary measures that might be used to increase private sector support,
- linkages to current information sharing systems,
- a link to the U.S. trade resumption protocols in the Maritime Infrastructure Recovery Plan.

The Result

While the overall evolution of the strategy and its supporting plans has been time-consuming, stretching from inception with the SAFE Port Act to the final release of the documents and careful development of fully informed implementation plans, the end result will reflect the care taken to craft it.

Just as the global supply chains are tremendously complex, ensuring they are secure, efficient, and resilient has necessitated diligent study, consultation, and consideration.



About the authors:

Ms. Maranda Sorrells is a policy analyst for the DHS Office of Transportation and Cargo Policy Development. Previously, she served as a DHS policy fellow after earning a master's degree in public policy from the University of Maryland. As a fellow, she worked at the DHS Privacy Office and U.S. Customs and Border Protection. She is currently the policy lead for surface transportation security issues.

Mr. Mike Callahan is a program analyst for the U.S. Coast Guard Office of Emerging Policy. In his current assignment he coordinates with interagency partners to develop national strategy and policy documents. He is a retired Coast Guard commander with an extensive background in Coast Guard operations.

Mr. Sean Moon is a senior policy advisor in the Office of Transportation and Cargo Policy Development in the Office of Policy at the U.S. Department of Homeland Security. A retired U.S. Coast Guard Commander, he chairs the Asia-Pacific Economic Cooperation Transportation Working Group Sub-Group for Maritime Security, and heads recurring delegations to APEC and other multilateral organizations on trade recovery issues. He is also the policy lead for the DHS small vessel security strategy.

For more INFORMATION:

For further information on the national strategy or its implementation, please visit the DHS website,

www.dhs.gov

During the second phase efforts, details on how you can be involved in the consultative process will be announced there.

The DHS Secure Supply Chain Initiative

Engaging the global community.

MR. SEAN K. MOON
Senior Policy Advisor
U.S. Department of Homeland Security

CAPT KEVIN KIEFER
Chief, Office of Port and Facility Activities
U.S. Coast Guard

by Ms. KEMBA ENEAS WALDEN
Director, Transportation and Cargo Policy
Office of Policy, U.S. Department of Homeland Security

In January 2011, U.S. Department of Homeland Security Secretary Janet Napolitano launched the Secure Supply Chain Initiative (SSCI), a program that seeks to enhance the security, efficiency, and resiliency of the transport systems and pathways that make up the global supply chain by developing cost-effective enhanced security measures and harmonized international guidelines and standards. The effort includes strengthening air, land, and sea pathways across global supply chain transport system facilities, conveyances, and cargo.

Within the initiative, governments collaboratively support the efforts of multinational organizations with relevant responsibilities, and advance key issues through active engagement and leadership. Specifically, stakeholders are encouraging the World Customs Organization (WCO), International Civil Aviation Organization (ICAO), the Universal Postal Union (UPU), and the International Maritime Organization (IMO) to develop new security measures and advance global guidelines and standards that are applicable to all modes of transport.

Recognizing that the Secure Supply Chain Initiative called for an international effort, Secretary Napolitano

met with the heads of multinational organizations to foster a broad coalition and elicit their active engagement.

Goals

Stakeholders are working to advance a coordinated and common agenda through three main goals, delineated as follows.

Prevent Exploitation. The first goal focuses on efforts to prevent terrorists from exploiting the supply chain's vulnerabilities. This means preventing attempts to use the supply chain as an attack mechanism or to illegally transport or gain access to weapons and materials, such as precursor chemicals that are used in improvised explosive devices or other potentially dangerous materials that could be used in an attack.

The global community is working to track the movement of known or suspected terrorists across international borders as well as to monitor products and technologies that can be used to make weapons. Doing so requires an effort to improve international standards, expand joint investigations and interdiction opera-

continued on page 24

International Focal Points

The international community has collaboratively identified and is implementing a number of objectives.

Identifying and responding to evolving threats and risks. Threats that could undermine or disrupt the global supply chain are constantly evolving. The global community is working to develop common understandings of system risks, common approaches to address those risks, and creating agile cooperative systems to identify and address emergent risks.

Work is ongoing within the WCO and ICAO to establish common definitions for elevated and high-risk cargo and to establish a common understanding of threats among customs and transport security authorities.

The WCO approved a risk management compendium that provides a foundation for national-level approaches to risk management, and provides guidelines to support risk assessment and targeting. Additionally, the ICAO has committed to developing a risk context statement to provide a similar foundation for the aviation environment.

The U.S. championed an emerging global threats working group to identify multi-lateral responses to emergent global enforcement threats.

On the maritime security front, the U.S. Coast Guard worked with the IMO to develop implementation guidance designed to enhance member state compliance with the International Ship and Port Facility Security code. This guide will help contracting governments promote maritime security by developing legal frameworks, managing associ-

ated administrative practices, and gathering technical materials and human resources necessary for compliance.

Updating timely and accurate advance information across all transportation modes. Analyzing information about goods moving in the global supply chain and the entities involved in these transactions allows government authorities to focus resources on the greatest threats and facilitate delivery of lawful shipments. Targeting is only as good as the information upon which it is based, so timely and accurate information is needed.

The WCO approved revised advance data guidelines for its framework of standards to secure and facilitate global trade. Informed by the U.S. Importer Security Filing (better known as the “10+2” rule), the new data guidelines include information elements negotiated between the public and private sectors over multiple years.

The WCO and ICAO have agreed to develop global guidelines for advance information for air cargo, focused in particular on the vastly increased speed of aviation, compared to maritime cargo.

Streamlining “Trusted Trader” programs. The WCO/ICAO technical experts working group is developing global guidelines for the wide array of regulator-to-business programs that exist across all modes of transport. This will help ensure consistency among customs and transportation security authorities, enhance efficiencies, and minimize impact on industry. In harmony with this effort, DHS is working domestically to increase the compatibility of domestic aviation and customs “trusted trader” programs.

Stemming the flow of illicit shipments of dangerous materials. The global supply chain is not only an attractive target for potential terrorist attacks, it is also vulnerable to exploitation by those seeking to transport dangerous material. International collaboration and establishing international legal instruments are needed to ensure that all nations have the resources, capabilities, and legal authorities to combat the exploitation of the supply chain.

In early 2010, interested stakeholders initiated Project Global Shield, an unprecedented, multi-lateral law enforcement effort aimed at combating the illicit diversion and trafficking of precursor chemicals for making explosives by monitoring their cross-border movement. As part of the SSCi effort, the World Customs Organization council approved the transition of Project Global Shield into a long-term program. Founded in cooperation with the WCO, INTERPOL, the United Nations Office of Drugs and Crime, and partner nations, the collaborative undertaking will focus on investigations, identifying and interdicting falsely declared precursor chemicals, and uncovering smuggling networks.

With respect to nuclear security, interested stakeholders are working with the International Atomic Energy Agency to develop strategic recommendations for United Nations member states to establish or improve nuclear security regimes and to carry out effective strategies to deter, detect, and respond to criminal acts with nuclear security implications. These efforts involve implementing the DHS Global Nuclear

Detection Architecture effort, identifying the means to share analysis, developing global standards for detection devices, and publishing global guidelines.

Securing and facilitating air cargo and global mail. After the attempted air bombing of two U.S.-bound cargo planes in October 2010, the global community has re-doubled efforts to secure air cargo and international mail.¹

- Work is ongoing with the Universal Postal Union (UPU) to develop advance data requirements for global mail, as U.S.-led operational pilots began in summer 2011 to provide information and recommendations.
- A 24/7 emergency contact mechanism is being developed to create security contacts in all UPU countries to adjudicate potential transit alarms through a UPU-established global mail sub-working group that includes WCO, ICAO, DHS, and U.S. Postal Investigations Service members.
- Efforts are ongoing in the UPU to develop international mail screening standards to resolve anomalies detected at international transit hubs.

Building resilience throughout the global supply chain. The global supply chain system must continue to function and be able to quickly recover from major disruptions. The Asia-Pacific Economic Cooperation, the IMO, the WCO, and the ICAO, are working to detail existing maritime centric frameworks into processes and policies for all modes of transportation. In the desired end state, these mechanisms will form the basis of WCO guidelines

and international capacity-building efforts that foster collaboration among governments and between government and the private sector.

Exploring and deploying new technologies. Modern technology plays a critical role in ensuring the security and efficiency of the global supply chain. Global guidelines and standards for technology ensure deployment of compatible and effective systems and processes, and encourage continued technical innovation. As such, the SSCi is emphasizing efforts to employ—and develop—modern technologies to achieve secure supply chains.

- Testing radiological/nuclear detection technologies is ongoing by DHS and the European Commission to identify those that meet internationally recognized standards promulgated by the American National Standards Institute and the International Electrotechnical Commission. Recommendations regarding any shortfalls in the current standards will be provided to the standard-setting bodies.
- To harmonize U.S. import information in pursuit of a single-entry window for industry, also known as CBP's International Trade Data System (ITDS), the U.S. is providing perspectives as a reference for other WCO member states and committing to continued U.S. leadership to develop proposed recommendations.

Bilateral Partnerships. In addition to identifying and implementing the objectives of the SSCi, DHS is working regionally and bilaterally with strategic partners to encourage their support of key action items within

the multinational organizations, and to develop joint declarations that will build international momentum of the initiative. These statements identify areas of mutual interest that can be advanced within the multinational organizations, and develop a framework for bilateral implementation. These statements explicitly support the work of multinational organizations to:

- develop new security measures and advance global best practices, guidelines, and standards to deliver security and trade facilitation;
- encourage an integrated, intermodal approach to ensure that the measures and standards developed within these international organizations are compatible to all modes of transport within the supply chain—air, land, and sea;
- support building bridges between the multinational organizations to enhance collaboration and reduce system vulnerabilities;
- push forward international standards aimed at strengthening global supply-chain security, including appropriate security controls at all stages of the chain; and
- promote and support capacity building.

Endnote:

¹ "Yemen-based al Qaeda group claims responsibility for parcel bomb plot," www.cnn.com.



tions, and strengthen the targeting and screening of potentially dangerous shipments worldwide.

Protect the Supply Chain. The global community is focusing on strengthening the critical infrastructure of the system across all modes of transport—air, land, and sea—against attack or disruption, along with precautionary procedures in place to reduce the risk of the supply chain being exploited by terrorists. Governments are focusing on building capacity for the most critical hubs and elements of the supply chain’s infrastructure to strengthen the security of the system as a whole.

Bolster Resilience. The third goal is to support the supply chain so that it can recover quickly in the event of a disruption. Ensuring the global supply chain can rebound rapidly, and ultimately with as little permanent disruption as possible, is critical to minimizing economic damage.

Until now, efforts primarily focused on response activities. The key to the current approach is the recognition that trade recovery activities must occur in conjunction with a large number of other actions related to incident response and to security. Many of these activities exist in the pre-event environment.

Such “steady state” systems need to be built with an eye toward all-hazards post-event needs. For instance, information collected for routine security needs can often be useful in managing trade flows when sys-



In her remarks to the WCO, Secretary Napolitano outlined the progress made with regard to the Supply Chain Security Initiative and emphasized the critical importance of continued collaboration. All photos courtesy of the World Customs Organization.

tems are disrupted. Further, resilience considerations in the pre-event environment must include issues of redundancy for transport systems and sources of supply. Coordination among trading partners is necessary to enhance resilience in this way (see sidebar).

On the Horizon

The goods, conveyances, and facilities that comprise the global supply chain system represent the engine of today’s global economy. Operating throughout the air, land, and sea environments—and frequently



Delegations from the customs administrations of the World Customs Organization met in council on June 23, 2011, in Brussels, Belgium. The WCO is the only international intergovernmental organization that deals with customs procedures governing trade between countries. It works to improve the effectiveness and efficiency of customs administrations across the globe, and helps to fulfill their roles of facilitating trade while ensuring its security.



World Customs Organization Secretary General Kunio Mikuriya led the June 23, 2011 council session in Brussels, Belgium. The broadly attended session was especially noteworthy, as it clearly demonstrated the commitment of multinational organizations such as the International Maritime Organization, the Universal Postal Union, and the International Civil Aviation Organization to cooperate and collaborate toward increasing global supply chain security, efficiency, and resiliency in all modes of transportation.

spanning two or all three in a single shipment—the system is complex and subject to unpredictable and potentially catastrophic events, including terrorist acts and natural disasters. It requires close integration to ensure seamless security, optimize efficiency, and create resilience.

Such integration is the responsibility of the public and private sectors, as they work to prevent the system from being disrupted or exploited. As such, it is incumbent upon the relevant regional, multilateral, and individual stakeholders to collaborate.

Through support of the SSCi, DHS and the international community are engaged in doing just that: strengthening the global supply chain to ensure it remains secure, efficient, and resilient through harmonized processes, procedures, and standards.

About the authors:

Mr. Sean Moon is a senior policy advisor in the Office of Transportation and Cargo Policy Development in the Office of Policy at the U.S. Department of Homeland Security. A retired U.S. Coast Guard Commander, he chairs the Asia-Pacific Economic Cooperation Transportation Working Group Sub-Group for Maritime Security, and heads recurring delegations to APEC and other multilateral organizations on trade recovery issues. He is also the policy lead for the DHS small vessel security strategy.

CAPT Kevin Kiefer serves as chief of the Office of Port and Facility Activities at U.S. Coast Guard headquarters. He co-chaired the International Maritime Organization correspondence group for the user guide to SOLAS Chapter XI-2 and the ISPS Code, and is the Coast Guard lead for the DHS secure supply chain initiative.

Ms. Kemba Walden is the director of Transportation and Cargo Policy Development in the Office of Policy at the U.S. Department of Homeland Security. Ms. Walden is leading a cross-component policy team to develop DHS's policy on wind farms, in addition to leading the department's efforts to develop a national strategy for global supply chain security. She was a chief organizer of the Air Domain Awareness effort, and served on a team to develop DHS's space policy. Ms. Walden was an international trade attorney specializing in export controls and foreign direct investment, prior to joining Homeland Security.



**U.S.
COAST
GUARD**

U.S. Coast Guard photo
by Cory J. Mendenhall.

International Maritime Organization User Guide

Managing risks to enhance maritime security.

by CAPT KEVIN KIEFER
Chief, Office of Port and Facility Activities
U.S. Coast Guard

MR. MARC MES
Director, Maritime Security
Canadian Coast Guard

In May 2011, the Maritime Safety Committee of the International Maritime Organization (IMO) approved the IMO user guide for SOLAS Chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code, which is a consolidated source of IMO maritime security-related material, intended to assist government officials, port facility employees, shipping company employees, and mariners with their security responsibilities.¹

The guide is designed to explain the security-related aspects of the International Convention for the Safety of Life at Sea (SOLAS) and assist SOLAS contracting governments in implementing, verifying compliance, and enforcing the provisions of SOLAS Chapter XI-2 and the ISPS Code.

In addition, it serves as an aid and reference for those engaged in delivering capacity-building activities in the field of maritime security. Ultimately, this will improve the security of global supply chains.

The IMO user guide is presented in five sections:

Section 1 **Section 1, "Introductions,"** describes the guide's purpose and content, provides an overview of security measures, outlines the benefits and challenges of implementing these measures, and explains the need to maintain security awareness.

The user guide promotes maritime security by providing guidance to governments, port facilities, port operators, ship owners, and ship operators on:

- setting security levels;
- managing risk consistently;
- establishing company security, port facility security, ship security officers;
- conducting port facility security assessments;
- developing ship security plans;
- establishing a system for security incident reporting;
- establishing the boundaries of a port facility.

Section 2 **Section 2, "Security Responsibilities of Governments and their National Authorities,"** provides guidance for the responsibilities of government officials, including:

- ◆ conducting port facility and ship inspections,
- ◆ establishing ship security communications,

- ◆ taking enforcement actions,
- ◆ training government officials with security responsibilities,
- ◆ ensuring national oversight,
- ◆ sending information to the IMO,
- ◆ implementing general port security measures.

Section 3 **Section 3, “Security Responsibilities of Port Facility and Port Operators,”** provides guidance for port facility and port operator duties, including:

- ◆ establishing a security framework;
- ◆ setting security levels;
- ◆ conducting port facility security assessments;
- ◆ drafting, reviewing, and implementing port facility security plans;
- ◆ establishing a port security baseline.

Section 4 **Section 4, “Security Responsibilities of Ship Operators,”** includes guidance on:

- ◆ changing security levels;
- ◆ training ship security personnel;
- ◆ establishing and maintaining ship security communications systems such as ship security alert systems, Automated Information Systems, and long range identification and tracking;
- ◆ conducting ship security assessments;
- ◆ drafting and submitting ship security plans;
- ◆ documenting security actions such as declarations of security;
- ◆ reporting security incidents.

Section 4 is applicable to operators of:

- ◆ passenger ships, including high-speed passenger craft carrying 12 or more passengers;
- ◆ cargo ships of 500 gross tonnage and upward, including high-speed craft, bulk carriers, chemical tankers, gas carriers, and oil tankers;
- ◆ mobile offshore drilling units (while underway);
- ◆ special purpose ships over 500 gross tons such as research and survey ships, training ships, fish processing and factory ships, salvage ships, cable and pipe laying ships, diving ships, and floating cranes.

Section 5 **Section 5, “Framework for Conducting Security Assessments,”** describes the security assessment methodology for port facilities and ports.

The section explains how to:

- ◆ establish assessment terminology and conduct a pre-assessment by creating a risk register;
- ◆ conduct a threat assessment and prepare threat scenarios;
- ◆ assess impact from a variety of types and magnitudes of events;
- ◆ identify asset vulnerability;
- ◆ score risk in a quantitative, systematic, repeatable way;
- ◆ manage risk by addressing weaknesses throughout the process.

Outreach

To promote capacity building, user guide outreach and training is under development. A variety of funding possibilities to conduct this training are being explored, which will allow the IMO to export training to port facilities as well as create a mix of online and on-site courses.

About the authors:

CAPT Kevin Kiefer serves as chief of the Office of Port and Facility Activities at U.S. Coast Guard headquarters. He co-chaired the International Maritime Organization correspondence group for the user guide to SOLAS Chapter XI-2 and the ISPS Code, and is the Coast Guard lead for the DHS secure supply chain initiative.

Mr. Marc Mes serves as director of Maritime Security for the Canadian Coast Guard. He served as co-chair of the IMO Correspondence Group for the user guide.

Endnotes:

¹ International Ship and Port Facility Security Code.

For more INFORMATION:

The user guide will be available at:
<http://www.imo.org/Publications/Pages/Home.aspx>

The user guide is available in its approved, working paper format at:
www.homeport.uscg.mil/mtsa
 in the “toolbox” section.

The Asia-Pacific Economic Cooperation

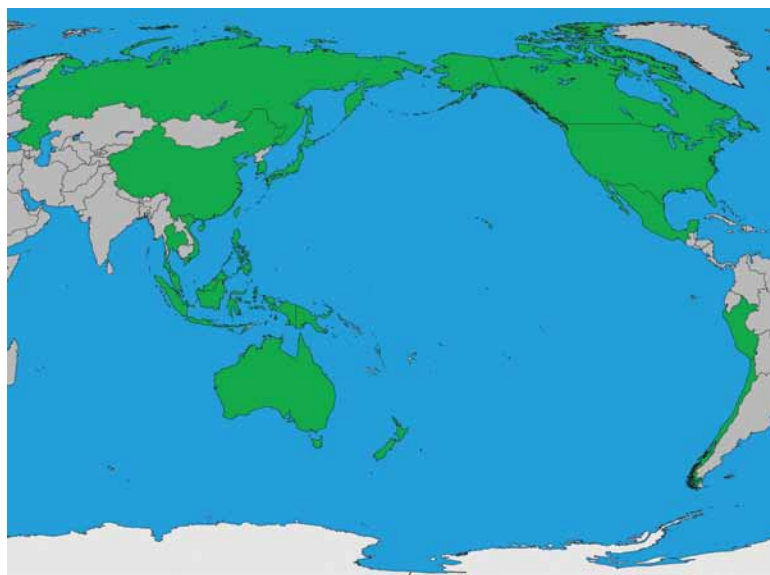
Regional efforts that support global solutions.

by MR. SEAN K. MOON
Senior Policy Advisor
U.S. Department of Homeland Security

The Asia-Pacific Economic Cooperation (APEC) is a forum of Pacific Rim countries dedicated to supporting sustainable economic growth and prosperity in the Asia-Pacific region. It was created in 1989 by 12 countries (including the United States) and has grown to include 21 members that account for 55 percent of global gross domestic product, purchase 58 percent of U.S. goods exports, account for 43 percent of world trade, and comprise a market of 2.7 billion consumers.¹ As a regional international organization, the 21 APEC member economies² cooperate in a fashion that engages government and private sector representatives at all levels to find solutions that enhance economic vitality. The organization is consensus-driven and lacks regulatory authority, ensuring that its work is fully cooperative. The end result is the collaborative increase in safety, security, and efficiency that can frequently serve as a model for other regional bodies and the international community.

APEC activities, including a secretariat in Singapore and various projects that support APEC's economic and trade goals, are centrally funded by yearly contributions from members. Since 1999 these contributions have totaled \$3.3 million each year, though from 2009 onward, member contributions will increase by 30 percent to a total of \$5 million each year.³ Since 1997, Japan has provided additional funds—between \$1.6 and 4.6 million annually—for projects that support trade and investment.⁴

Any APEC committee, sub-forum, working group, task force, or dialogue group may propose a project. These proposals are vetted by appropriate subject experts in committee and are ranked, prioritized, and



APEC members include Australia, Brunei Darussalam, Canada, Chile, the People's Republic of China, Hong Kong China, Indonesia, Japan, the Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Vietnam.

(where appropriate) endorsed for further review by secretariat personnel. Final approval authority rests with the Budget and Management Committee or by senior officials if a project request exceeds \$200,000.

The APEC Maritime Security Sub-Group (MEG-SEC) takes the lead with regard to maritime security-related projects. Typical APEC projects include seminars, publications, research, and workshops, and are open to participation from all member economies.

continued on page 31



The Phases

To promote sustainability, the MEG-SEC adopted a three-phase approach to delivering assistance to beneficiary economies:

Phase I: The ICIAP Phase I focused on raising awareness of ISPS Code requirements and assisting developing economies with building a framework for implementation. Phase I workshops were held from March 2005 to June 2006 in the Philippines, Thailand, Indonesia, Vietnam, Peru, and Malaysia. The United States led the workshops in Peru and the Philippines; Japan led the workshops in Vietnam and Malaysia; and Canada led the workshop in Thailand.



Representatives from the Indonesia Coast Guard run a risk-scoring scenario through the Port Security Risk Assessment Tool during a training workshop. USCG photo by Mr. Thomas Kalisz.

Phase II: Ongoing ICIAP Phase II activities focus on building the capacity of developing economies to conduct ISPS Code compliance-related drills, exercises, and assessments. Phase II activities are tailored to the operational needs of maritime security personnel in the beneficiary economy. The drills and exercises build capacity toward more effective ISPS Code implementation and assist economies in developing quality control measures to ensure that progress is sustained. Similarly, the international version of the U.S. Coast Guard's Port Security Risk Assessment Tool, along with training on its implementation and use, assists economies with resource allocation and fosters risk-informed security processes.

ICIAP Phase II initially consisted of a second round of workshops held in Vietnam, Indonesia, Thailand and Papua New Guinea. As a follow-up to the Canada-led Phase I workshop in Thailand, Thai officials visited Canada to learn about their port security activities. A pilot model visit (precur-

sor to ICIAP Phase III activities) led by Australia was conducted in Papua, New Guinea, in October 2007.

Workshops consisted of presentations, discussions, table-top exercises, and on-site visits to port facilities. Geared toward operational port facility security personnel, the efforts focused on practical aspects of ISPS Code implementation, eschewing theoretical or awareness training geared toward government or facility management personnel. Specific topics were adjusted to meet the needs of the individual economies, but in general included command, control, coordination and communications (C4) procedures, coordination processes with external security agencies, discussion of enhancement measures for increasing security levels, and audit techniques.

As part of Phase II, MEG-SEC members determined that developing a manual for conducting standardized drills and exercises would be useful. A questionnaire related to conducting drills and exercises was developed and circulated to member economies by the MEG-SEC chair and a manual was presented for



Trainees conduct a vessel boarding and container security sweep exercise based on the APEC drill and exercise manual following a workshop held in Manila, Philippines. USCG photo by Mr. Thomas Kalisz.

approval at the 30th meeting of MEG-SEC, held in Manila, Philippines, in April 2008.

Demonstrating how APEC projects can have global impact beyond the Asia-Pacific region, the MEG-SEC partnered with the United States, Canada, and the



Members of the Asia-Pacific Economic Cooperation Maritime Security Sub-Group discuss methods to enhance regional implementation of the IMO ISPS Code through capacity building efforts among member economies. Photo courtesy of the Australian Office of Transport Security, Department of Infrastructure and Transport.

Organization of American States (OAS) to translate the APEC drill and exercise manual into Spanish and sponsor workshops in Latin and South America. To date, 280 participants from 45 countries and APEC economies have participated, creating a wide-ranging global standard for drills and exercises.¹

A pilot workshop was held in early 2010, in Peru, to deliver an international version of the U.S. Coast Guard's Port Security Risk Assessment Tool (PSRAT) and provide training on its use. The workshop introduced risk assessment methodologies and was followed by hands-on training with the software. This initial workshop was the genesis of expanded deployment of the tool to Thailand, Indonesia, and Vietnam in 2010 and 2011.

The PSRAT itself is a relative risk-ranking tool that enables users to assess infrastructure risks across geographic regions. Users assess consequences, threats, and vulnerabilities for specific attack scenarios on designated infrastructure. These subjective evaluations generate quantitative risk values of use in identifying critical infrastructure, estimating countermeasure effectiveness, defining risk management strategies, and allocating resources.

Phase III: ICIAP Phase III activities (also ongoing) include the port security visit program (initiated as the pilot model visit) and self-assessment training workshops.

Endnote:

¹ Maritime Security Sub-Group Final Report from the 33rd APEC Transportation Working Group Meeting, Tokyo, Japan, October 2010.

In 2010, the Budget and Management Committee approved 99 APEC work projects ranging from improving trade agreement development, sharing best practices, and capacity-building to addressing security issues. The projects were valued at around \$9 million and spanned all 21 member economies.⁵

ISPS Code Implementation Assistance Program

The International Ship and Port Facility (ISPS) Code Implementation Assistance Program (ICIAP), which began in 2005, demonstrates the cooperative nature of the organization, particularly noteworthy in the maritime security realm. Annual project proposals have continued ICIAP efforts, with further refinements and additional capacity-building efforts anticipated into 2012 and beyond. The ICIAP assists APEC economies to develop the capacities necessary to effectively implement the ISPS Code. The program scope encompasses a transfer of knowledge, lessons learned, best practices, and tools to help economies implement and foster risk-informed security regimes.

Expanding Emphasis to Focus

Enhanced Capacity

At a meeting of the APEC Transportation Working Group in Brisbane, Australia in mid-July 2011, the MEG-SEC reviewed the results of the ICIAP and assessed common trends in ISPS Code compliance and identified several common themes, including:

- access control,
- cargo screening,
- drills and exercises,
- auditing,
- legislation,
- information sharing,
- port/ship interfaces.

Each was discussed in detail, noting that information was somewhat limited, and due to its multi-year nature, could only be considered representative of areas for consideration.⁶

The group determined that, in addition to the ongoing efforts of the ICIAP, which were believed to satisfy a number of the themes, additional emphasis was necessary to further regional maritime security. Suggestions include:

- Conducting a workshop or series of workshops to enable economies to exchange implementation options in each identified thematic area. This project will complement the IMO's



The Port Security Visit Program

This program is focused on the maritime security requirements under the ISPS Code, with the aim of identifying the needs an economy may have in achieving and maintaining its obligations under the code. Strictly voluntary for APEC economies seeking to identify strengths and weaknesses in their implementation of the code, the program facilitates regional expert visits to ports under pre-negotiated terms of reference.

This enables APEC economies to:

- share experiences on best practices and lessons learned within the region;
- identify future areas of cooperation and capacity building as a basis for planning future phases of the ICIAP, with the understanding that all information gathered and produced during a visit remains the property of the host economy;
- create a pool of regional expertise on implementation practices;
- achieve greater consistency in ISPS Code implementation practices and progress;
- strengthen cooperative relationships;
- promote a common understanding of maritime security issues; and
- achieve a systematic, risk-based review of a participating economy's ISPS Code implementation framework, practices, and progress to date.

recently approved user guide to SOLAS chapter XI-2 and the ISPS Code, with a goal of developing an eventual APEC publication to assist economies with implementation practices.

- Revising the APEC drill and exercise manual and updating it with lessons learned keeps the document relevant. Additional exercise scenarios will be added, including scenarios geared toward smaller economies with less governmental infrastructure and one designed specifically for senior leadership.
- Developing a model legislation workshop to organize the ISPS Code and add areas of emphasis currently lacking, such as incident response and enforcement. The project will include a beta test workshop, with an eye toward future discussions to promote all-encompassing legislative regimes harmonized across the Asia-Pacific region.

The U.S. Coast Guard also provided the MEG-SEC with a presentation on its Common Assessment Reporting Tool (CART), a system that provides an online repository of maritime transportation system recovery information. CART provides timely and accurate pre-incident data and allows comparison of that information to post-incident data to characterize impact to transportation systems, prioritize recovery action, and manage trade resumption efforts.

The Coast Guard routinely uses this Web-based tool, which has been refined during multiple recent disasters. A version of CART has recently been approved for distribution internationally and a workshop was held in Thailand in early June 2011, to gather information related to further international sharing. It is anticipated, especially after the recent series of natural disasters in the Asia-Pacific region, that deployment will be on-going and rapid.

Ongoing Efforts

In 2006, APEC senior officials endorsed an initiative to address coordinating trade flows in the aftermath of a transportation system disruption. In 2007, 10 economies under the leadership of Singapore worked together to create guidelines to facilitate the restoration of trade among APEC economies as rapidly as possible after a terrorist attack and to promote actions to facilitate trust and confidence in the process. The framework was then validated in 2008 through a closely scripted set of exercises involving economies exchanging necessary information and harmonizing economic and security priorities.

The World Customs Organization (WCO) also noted in 2008 a similar need to enhance trade resilience on the broader world stage. With the support of the APEC economies, the WCO used the APEC Trade Recovery Programme as a basis for developing trade recovery guidelines to support its Framework to Secure and Facilitate Global Trade. While slightly different in emphasis (for instance, the WCO guidelines include a greater emphasis on communications mechanisms) the two efforts show an evolutionary linkage.

APEC continues to support WCO trade recovery efforts as the SAFE Framework of Standards is reviewed and revised and the trade recovery guidelines are further detailed. Through a Secure Trade in the APEC Region (STAR) conference sponsored by the United States in its role as an APEC host economy, trade recovery information exchange was discussed among the economies and with the private sector to develop consensus on what information elements are necessary for government-to-government and government-to-private sector dialogue. A report of the conference breakout session will be provided to the WCO to help inform its efforts.

Secure, efficient, and resilient supply chains, including their maritime elements, are an inherently global effort. Through capacity building initiatives, such as those conducted by the Asia-Pacific Economic Coop-

eration that assist developing nations implement international standards and enhance coordination and harmonization among nations, such efforts can achieve local solutions with regional impact. And such regional efforts can further inform broader, global solutions.

APEC is realizing just such solutions—creating a more secure transportation system through collaboration and consensus through the work of the MEG-SEC.

About the author:

Mr. Sean Moon is a senior policy advisor in the Office of Transportation and Cargo Policy Development in the Office of Policy at the U.S. Department of Homeland Security. A retired U.S. Coast Guard Commander, he chairs the Asia-Pacific Economic Cooperation Transportation Working Group Sub-Group for Maritime Security, and heads recurring delegations to APEC and other multilateral organizations on trade recovery issues. He is also the policy lead for the DHS small vessel security strategy.

Endnotes:

1. Asia-Pacific Economic Cooperation, 2011. www.apec.org.
2. Termed “economies” due to the APEC cooperative process focus on economic and trade issues, APEC members include seven of America’s top 15 trading partners.
3. All figures are reported in U.S. dollars.
4. Asia-Pacific Economic Cooperation, 2011. www.apec.org.
5. Ibid.
6. Maritime Security Sub-Group Final Report from the 34rd APEC Transportation Working Group Meeting, Brisbane, Australia, July 2011.



International Port Security

A global challenge.

by LT DAN ORCHARD

Africa Desk Officer

U.S. Coast Guard International Port Security Program

Travel the world as any mariner has and one may discover that what qualifies as port security can span a spectrum as broad as a country's cuisines. Security practices in some ports may appear to be impenetrable, with perimeters fortified by armed soldiers posted in observation towers and electric fences amped with enough juice to drop an unwary animal. While, in other locations across the globe, children clamber through dilapidated fences to sell lunches to longshoremen.

Poor security practices in some nations may increase the risk of terrorist or criminal acts to the vessels that call on them, their trading partners, and the entire global maritime transportation sector. Since the world is connected by maritime trade, the Coast Guard recognizes that if it is going to protect U.S. ports, as well as maritime commerce as a whole, it needs to engage

with officials around the globe to heighten the level of scrutiny around their ship-to-port interface.

In 2004, the Coast Guard created the International Port Security (IPS) program to do just that. That same year, the International Maritime Organization (IMO) put into force the International Ship and Port Facility Security (ISPS) Code. Since then the IPS program has championed the ISPS Code by visiting more than 150 coastal nations, collaborating with foreign partners as they develop security systems around their centers of maritime trade and transportation.

Security practices throughout the world have made significant improvements. While many nations have implemented the ISPS Code and are ready to move beyond it, a handful are still struggling to sustain or simply embrace its fundamental principles.

History

In 2002, the U.S. Congress passed the Maritime Transportation Security Act, directing the U.S. Department of Homeland Security to learn about the anti-terrorism measures in place in foreign ports, and to offer training to countries where security standards appeared to be inadequate. DHS delegated this mandate to the Coast Guard, which formed the IPS program in 2004. By 2008, the Coast Guard had visited all of its trading partners at least once.

The program operates on the principle that a continuous exchange of ideas, observations, and personal visits is the most productive way to improve security on another's sovereign shore. Along this line, the Coast Guard dedicated a core of experienced members as international port security liaison officers to act as the conduit with foreign authorities by developing rela-



LCDR Daron Tanko, right, discusses port security with an official in a container facility in Angola. USCG photo by Mr. Thomas White.

tionships, understanding ambitions, and arranging supporting resources. At the center of this exchange is a formal visit when the Coast Guard sends a team of port security experts to the country for about a week to engage personally with their counterparts.

Upon arrival in a foreign country, the team meets with the designated authority—the agency responsible for overseeing port facility security—to discuss its overarching responsibilities of port security governance. Initial visits focused on how each country implemented the ISPS Code—a starting point for security and anti-terrorism measures. The ISPS Code was written with performance-based directives, such as “control access to the port facility” and “supervise the handling of cargo,” as opposed to mandating specific prescriptive actions such as fence heights or photo identification cards. The IPS teams observe how these agencies interpret the code and implement their standards.

From there, the teams meet with the security officers and authorities in the country’s major ports to view security practices in action with an eye toward the key principles of the ISPS Code, including:

- access control,
- restricted areas,
- cargo handling,
- delivery of stores/supplies,
- security monitoring,
- security policies and procedures,
- security training and exercises.

The ultimate goal of the IPS program is to foster the interchange of ideas and best practices. The Coast Guard invites host nations to travel to the U.S. to witness how the ISPS Code and other security measures are implemented here. More than 70 countries, or half of the world’s coastal nations, have taken up the offer. During their week in the U.S., foreign delegations are encouraged to interact with the Coast Guard and other government agency officials while touring facilities of a similar capacity and cargo design as their own.

Observations

IPS program personnel traveled abroad to more than 150 countries and learned that an overwhelming majority of the world’s coastal nations have substantially implemented the ISPS Code. Each country did this in its own particular manner. While the ISPS Code does not require the implementation of specific types of physical security measures, the IPS program



LCDR Eric May, left, discusses security guard procedures with a member of the gendarmerie while overlooking the port of Doula in Cameroon. USCG photo by LT Dan Orchard.

revealed that many countries draw upon a similar set of tools to secure their ports, including:

- a strong physical perimeter of walls, fences, and barricades;
- warning signs at entry points and along the waterfront;
- segregated entrances for pedestrians, cars, and trucks;
- identification cards with expiration dates, photographs, and color-coding for additional access to restricted areas;
- closed-circuit television systems;
- lighting with back-up generators;
- guards on patrol in vehicles or water craft and equipped with radios.

Port officials reported that implementing the ISPS Code resulted in tangible benefits beyond deterring terrorism. The improvements to physical security, combined with disciplined access control, have reduced access to containers and equipment and opportunities to board a vessel.

Additionally, tidy, well-lighted facilities, free from the congestion of unnecessary persons and vehicles, operate with increased efficiency, resulting in significantly improved cost savings. Benefits continue, as stricter cargo control works to improve customs declarations accuracy, which can lead to increases in revenue for the port. Tighter control of truck movements can reduce the number of motor vehicle accidents and the associated costs of down-time, investigations, and damage. Restricting facility access to authorized employees and guests may reduce the risk of criminal behavior.

Conditions of Entry

Vessels coming from insecure foreign ports can pose a significant threat to the U.S. and/or any other country that they call on. It is therefore very important to secure the entire supply chain, including the foreign ports.

The Coast Guard publishes a list of these countries in a port security advisory at www.homeport.uscg.mil. The effective date for the countries listed below was Oct. 14, 2011.

Under the authority of the Maritime Transportation Security Act, the U.S. Coast Guard imposed conditions of entry on vessels arriving to the U.S. from the following countries that do not maintain effective anti-terrorism measures:

Cambodia	Iran
Cameroon	Liberia
Comoros	Madagascar
Cote d'Ivoire	Sao Tome & Principe
Cuba	Syria
Equatorial Guinea	Timor-Leste
Guinea-Bissau	Venezuela
Indonesia	

During these visits, liaison officers collected many innovative practices as “best practices,” which they shared with other nations looking for effective, low-cost methods to address vulnerabilities. That said, a critical component of the ISPS Code is to test these practices, whether innovative or standard, through regular drills and exercises, so port officials can identify vulnerabilities and address them prior to an actual incident. IPS program officers learned that a common weakness among ports across the world has been this evaluation process. For some ports, it is a matter of apathy or lack of oversight. Others simply lacked the expertise or resources to conduct effective tests.

By reaching out to countries one-on-one or by coordinating with regional partners, such as the Asia Pacific Economic Cooperation Forum (APEC), the Organization of American States, and the Group of Eight, IPS program officers elevated this compe-

tency throughout the world. For example, IPS program personnel partnered with APEC and Transport Canada to create a manual for conducting drills and exercises that has been circulated to more than 85 countries.

Protecting U.S. Ports

If an overwhelming majority of the world’s coastal nations have substantially implemented the ISPS Code, then, unfortunately, a handful have not.

Since 2004, the IPS Program determined that a number of nations were unable to substantially implement, or sustain the core elements of the ISPS Code. In each instance, the Coast Guard worked closely with the country to resolve the derogatory issues. The country’s officials developed a plan of action to improve shortcomings, while the liaison officers supported their goals by providing specific training, compliance references from the IMO, and opportunities to tour U.S. facilities.

In several instances, this effort improved security and resolved many concerns. In other cases, however, countries were unable to integrate the necessary improvements, so the Coast Guard imposed conditions of entry on vessels arriving to the United States from ports that are not secure. Prior to allowing these vessels into a U.S. port, the Coast Guard normally boards or examines them to ensure that the master took additional security precautions while in the foreign port. As a result of the increased security

continued on page 38

IPS Program Ongoing Efforts in West Africa

The IPS program recently hosted West African delegations from Cameroon, Republic of Congo, Gabon, Gambia, Ghana, Liberia, Nigeria, and Togo and program personnel conducted training in Cameroon, Senegal, and Benin.

The IPS program continues to work with other U.S. agencies to improve port security in West Africa as well as in other countries that have not implemented the ISPS Code.

Trust But Verify

Port security information is extremely valuable to the world's port state control authorities and is generally unavailable through other means except the self-reporting of each individual country. The International Convention for the Safety of Life at Sea, which houses the ISPS Code in Chapter XI-2, does not authorize the IMO to audit member states to verify compliance.

Instead, compliance is determined by the country itself and then reported back to the IMO, which publishes the declaration on its website. Of IMO members, all but three reported compliance by 2008. The IPS program revealed that compliance was not so complete.

As of July, 2011, the Coast Guard had imposed conditions of entry on vessels arriving from several countries (see sidebar). While these countries span the globe, one region of the world emerged as having similar challenges in multiple nations. Over half of the countries with inadequate port security were in sub-Saharan Africa, and, more specifically, seven of the countries were in West Africa. This region also battles other significant maritime issues such as piracy, illegal fishing, pollution, and drug and human trafficking.

Some of the issues in this region extend beyond the control of the individual port authority, which is why the Coast Guard exempts specific ports from conditions of entry when they have shown that they have independently implemented effective anti-terrorism measures. In addition, it is unreasonable to expect some of these developing nations to have the resources and expertise to sustain comprehensive port security improvements without assistance.



LCDR Jose Perez, right, discusses waterside security measures with a security officer at a petroleum facility in Equatorial Guinea, Africa. USCG photo by LT Dan Orchard.



Mr. Michael Brown, chief, USCG International Port Security Evaluation Division, reviews a visitor log with officials in a port in Libya. USCG photo.

measures and scrutiny, the vessel incurs unwanted expenses and delays.

Beyond the ISPS Code

The Coast Guard views the ISPS Code as a minimum standard for securing a port. In many regards, it does not go far enough to address vulnerabilities or deter terrorist and criminal acts. For example, how does a vessel protect itself from a small boat attack like the one encountered by the *M/V Limburg*, on Oct. 6, 2002?¹

The U.S. has taken a holistic approach to port security by viewing the entire port as a collection of facilities through port security plans. In addition, area maritime security committees augment individual ship and port facility security plans by defining the responsibilities of the Coast Guard and other law enforcement agencies with regard to protecting critical maritime infrastructure.

Additionally, the IPS program shares information about some of the tools the U.S. uses to display a common operational picture, such as the maritime safety and security information system, Automatic Identifi-

cation System, long-range identification and tracking, and advance notice of arrival. The IPS program develops model port security legislation to assist countries that have yet to codify appropriate mandates in their domestic law.

The Coast Guard's intent is to work closely with trading partners and other international stakeholders to improve port security. Shaped by global threats and challenges, efforts to govern the maritime domain today reflect complex, interwoven mutual interests and actions. By working together, the overall security for the global maritime transportation system can be raised to a level that will deter the actions of those who intend to cause harm.

About the author:

LT Daniel Orchard is the Africa desk officer in the IPS program at Coast Guard headquarters. As a reservist, he was a founding member of Port Security Unit 301. He deployed to Iraq in 2009 to train the Iraqi Navy in small boat security zone enforcement.

Endnote:

¹ *M/V Limburg* was rammed by another boat off the coast of Yemen, resulting in damage to its hull and the death of one crewmember. Some oil escaped, but the vessel remained seaworthy.

China Coast Guard members welcome in the crew of the high endurance cutter *Boutwell*. The crew from the *Boutwell* represents the U.S. Coast Guard here and at other foreign ports to increase international maritime security and safety. Coast Guard photo by Petty Officer Jonathan Cilley.



Notice of Arrival and Departure

A link to maritime domain awareness and safety.

by LT SHARMINE JONES
*Advance Notice of Arrival Program Manager
U.S. Coast Guard Office of Vessel Activities*

The U.S. Coast Guard is the nation's steward in the prevention of terrorism by sea. As a part of the Department of Homeland Security, the USCG has been performing waterway security missions long before the terrorist attacks on the United States on Sept. 11, 2001.

One of the ways the Coast Guard is able to protect the nation is by requiring arriving vessels to provide a 24-hour notice of arrival and departure (NOAD). The Coast Guard evaluates vessel arrival information and schedules examinations of arriving vessels for compliance with international and domestic vessels safety and environmental protection standards. Shortly after September 11, the Coast Guard began making efforts to upgrade NOAD requirements from 24 to 96 hours; allowing more time to gather imperative information from arriving vessels.

The National Vessel Movement Center (NVMC), a subdivision of the USCG, is responsible for the collection of NOADs. It is staffed 24/7 to provide services including:

- ship arrival notification system data processing and reconciliation;
- customer support for NOAD submissions and regulations;
- help desk support;
- maritime search and rescue, law enforcement, and U.S. Coast Guard field support.

This subdivision processes approximately 7,000 NOADs weekly, 98 percent of them electronically. The data is then entered into the ship arrival notification system where it is analyzed by the intelligence

community and local captain of the port to identify higher risk vessels.

NOAD regulations apply to foreign and U.S. commercial vessels that are 300 gross tons or more, foreign recreational vessels 300 gross tons or more, and vessels carrying certain dangerous cargo. NOAD regulations do not apply to vessels less than 300 gross tons, unless the vessel is carrying dangerous cargo or operating in the Seventh District area of responsibility in South Carolina, Florida, Puerto Rico, and U.S. Virgin Islands, all of which have a large contingent of small commercial shipping vessels that must meet international and domestic shipping standards for safety and security. The Coast Guard conducts examinations on the vessels utilizing the Caribbean Cargo Ship Safety Code in accordance with the Caribbean Memorandum of Understanding on Port State Control.

The Coast Guard has proposed significant improvements to the notice of arrival and departure regulations. If adopted, the proposed changes will make the NOAD regulation apply to more vessels, as the 300 gross ton applicability threshold will be removed.

The NOAD Process

For industry, the process is relatively simple. The reporting party (agent, owner, operator, master, etc.) submits a NOAD. The vessel will receive a receipt stating that the National Vessel Movement Center received the NOAD and indicate if it is missing critical information. Once the NVMC processes the notice of arrival/departure, no further action is necessary from the reporting party, provided the information remains unchanged. If critical information is miss-

Ship Arrival Notification System

SANS utilizes four modules:

- 1** SANS, the central repository of NOAD data/information, is maintained by the USCG Operation Systems Center.
- 2** iSANS is internal to USCG; and is used by NVMC personnel to input and/or validate NOAD information and allows USCG personnel to view NOAD information.
- 3** SANS-DHS is the Web-based portal for DHS and other federal/state users who need access to NOAD information.
- 4** e-NOAD stands for the electronic NOAD, an external Web-based portal that enables regulated vessels to provide electronic submission of notice of arrival/departure information.

ing, the reporting party will be notified by an NVMC marine representative and then must submit a corrected NOAD.

Once NVMC processes it, the NOAD becomes available to the CBP, Coast Guard field personnel, the Intelligence Coordination Center, and the National Maritime Intelligence Center through the ship arrival notification system (SANS) user interface.

Creating an Information Chain

The USCG extracts information from SANS to assess the risk of vessels arriving or departing from a U.S. port and to identify vessels and individuals associated with those vessels who may pose a security or safety risk. The data is also retained for USCG trend analysis.

NOAD information is combined with other resources to form a common operational picture in which

vessel-specific information and movements within our ports and waterways are monitored in real time. This information is then used as a decision-making aid for field commanders and is often referenced in support of interagency and DoD efforts in homeland security, thereby improving our layered approach to safety and security through information sharing.



The Coast Guard conducts an at sea boarding prior to the vessel's arrival into an U.S. port. Security boardings can occur for a number of reasons, such as the vessel being a first-time caller to an U.S. port. All photos USCG.

An Interagency Alliance

The notice of arrival and departure serves the Coast Guard and other federal entities that share common interests and goals. For example, CBP published a rulemaking in April of 2005 mandating that all commercial vessels (regardless of tonnage) arriving in the U.S. from a foreign port submit crew and passenger information via the CG electronic NOAD application. CBP captures this information in its advanced passenger information system, and the data is then retrievable by their field agents. The Center for Disease and Control receives critical crew and passenger information, which can be used to identify health threats.

The NOAD intergovernmental cooperation includes a memorandum of agreement with the St. Lawrence Seaway Development (SLSDC) to collect notice of arrival information for vessels transiting to Canada through the seaway. The USCG has also worked with the islands of the Caribbean to assist in collecting pre-arrival information. In 2007, for example, the Caribbean hosted the Cricket World Cup, which garnered international attention. Since this was the first time an event of this scale was held in the Caribbean, security was a significant concern. Recognizing the need for a notification system for vessels arriving to the West Indies, a council consisting of delegates from the various Caribbean nations contacted the U.S. Coast Guard for assistance with developing a vessel notification system. Pending development of a system for the Caribbean region, an interim measure was put in place whereby the CG e-NOAD application was used to collect information for vessels operating in the Caribbean. A Caribbean notice of arrival system has since been developed; however, vessels still have the option to submit NOA information for the Caribbean region through the e-NOAD application.

For CG port safety and/or security issues, the NOAD is reviewed to determine whether inspections are required on a particular vessel, or if there is a need to establish safety/security zones, escorts, boardings, or other safety operations. Information is loaded into the Marine Information for Safety and Law Enforcement system (MISLE), which is used to store data on marine pollution, inspections results, and other shipping and port accidents in U.S. waters. The ship arrival notification system matches the vessel with its record in MISLE and attaches the MISLE unique vessel number so arrival information may be pulled into the MISLE arrivals page for ease of access.

NOAD in Action

For national security and screening purposes, CBP receives the notice of arrival and departure information in real time from SANS. This information can be shared with other federal and foreign government intelligence or counterterrorism agencies or components when the USCG becomes aware of a potential threat to national or international security, or to assist in anti-terrorism efforts.

Managing the Data

With more than 120,000 reports processed yearly, information in SANS is maintained for a period of no more than 10 years or when no longer needed (which ever is longer) from the date of collection. Additionally, the only notice of arrival and departure information retained initially is related to those individuals about whom derogatory information is revealed during the screening process. Should derogatory information be discovered by USCG either through the Treasury Enforcement Communication System or USCG's own sources, alerts and information are then communicated to the field.

As the Coast Guard and the Department of Homeland Security continue to move forward, regulations, policies, and programs like the NOAD help to keep our homeland secure and are vital components to ensure maritime domain awareness and safety. Today, information sharing is critical as more regulations and laws are enacted.



The Coast Guard conducts a port state control examination.

For more INFORMATION:

Visit

<http://www.nvmc.uscg.gov/NVMC/Default.aspx>

The NVMC receives an e-NOAD from a liquid natural gas (LNG) carrier arriving from Yemen, heading to Boston, Mass. This generates an automatic request for LRIT (long-range identification and tracking) information. Upon receipt of the LRIT information, the vessel can be tracked until it is within Automatic Identification System range.

Simultaneously, CBP and the USCG receive notification via their respective systems that this LNG carrier intends to arrive at a port in the U.S. Due to the highly flammable nature of the cargo, this vessel can potentially be a target for a terrorist attack. As the vessel approaches, the local CG sector detects, identifies, and tracks the vessel by correlating multiple data sources like the vessel's NOAD and electronic signal from its AIS.

With AIS and other sensors displayed in the common operational picture, the exact position of the vessel is known so that a Coast Guard boarding team or escort vessel and other local law enforcement assets can assist the vessel as it enters the port. While aboard the vessel, the boarding team may compare the crew list to the one submitted via the e-NOAD to determine if there are any anomalies. If the master cannot explain the anomaly, this may trigger control actions.

In this example, the vessel could be considered a terrorist target, but the presence of federal law enforcement agents and assets reduces its vulnerability. In addition, the Coast Guard uses the NOAD as a screening tool to target vessels for port state control examinations, examinations to ensure compliance with maritime security requirements, or for law enforcement boardings. Furthermore the Coast Guard will use the NOAD information to determine if a security zone or action is warranted.



The e-NOAD will continue to evolve and may become a part of a single Department of Homeland Security-sponsored window for reporting all arrivals and departures to the United States. By working together, government and private agencies can create a system that can facilitate commerce while serving a multitude of needs to reduce the industry reporting burden.

About the author:

LT Sharmine Jones is the advance notice of arrival program manager and assistant port state control program manager at Coast Guard headquarters. She has served at multiple field units, including Marine Safety Office Mobile, where she served as the facilities branch chief, assistant port state control branch chief, and vessels arrivals branch chief.



Keeping Cargo Moving

How marine terminals process supply chain data.

by CAPTAIN JEREMY SYKES
Account Executive
MDP Marine Insurance

MR. ED MERKLE
Director of Port Security and Emergency Operations
Virginia Port Authority

Competition is on the rise in shipping ports around the world; so terminals must be efficient and effective to keep business flowing. Ship lines don't make money when vessels are at a terminal; therefore, the terminals want to hold the ships for the shortest time possible.

However, the ship-to-shore terminal operating system is not the source of a container terminal's main bottlenecks, as these normally occur in the transfer system and delivery-receipt system. Information technology helps terminals handle and process the data within the supply chain to alleviate these bottlenecks, increase overall performance, and ensure ship lines sail on schedule.

While container terminals, as interfaces among various modes of transport, possess a great deal of physical assets, they also use a large amount of computerized software. A well-designed computerized container control system helps terminals provide:

- faster container loading and discharging,
- improved container yard monitoring,
- reduced number of container re-handles and shifts,
- increased information accuracy,
- decreased workload on terminal staff,
- improved ability to track movements in real-time,
- better container slot scheduling.

A broad scope of options for the container terminal operator to computerize its supply chain management system can vary, from a basic data entry and

retrieval system to an advanced multisystem approach using a real-time operation system. The proper information system can control the entire supply chain to eliminate bottlenecks, manage cargo, and allow synergies across the various nodes.

Terminal Operating Systems

Terminal operating systems help terminal operators to better manage the copious amount of information associated with cargo handling, and help them to increase terminal performance and capacity of the terminal without expanding the terminal's physical footprint.



Photo courtesy of the Port of Virginia.



History of Container Terminal Systems

In the past, terminal operators utilized paper-based administration systems to plan, control, and record the movement and storage of containers. The terminal staff often communicated via two-way radios and visually confirmed and tracked shipments.

By the mid-1970s, many terminal operators used basic computer systems that allowed them to perform data transmissions, use database management systems, and conduct computer processing. With advances in technology, terminal operators began to develop software to incorporate the various sub-systems of a container terminal operation, including:

- ship to shore—movement of containers from ship to berth;
- transfer cycle—movement of containers from berth to stack (storage area);
- storage—stack or area where containers are placed;
- delivery/receipt—movement of containers from stack to the gate.

The terminal operating systems helped a terminal operator access real-time data, container reports, and container inventory locations. By the early 1980s, approximately 78 percent of container terminals used computerized administration systems and more than 40 percent were using terminal operating systems to manage landside and marine operations.

When information is received into the computer system, it is stored in a database and is either sent out or accessed by users of the system on the terminal. Some of the technologies and electronic devices that support this system include:

- radio frequency identification devices (RFIDs), which use radio waves to transfer data between a reader and an electronic tag attached to an object to identify and track the object;
- optical character recognition, in which a scanner reads printed characters;
- wireless local area network handheld computers with built in RFID scanners;
- global positioning system (GPS) devices.

The Future of Terminal Operating Systems

Within the past several years, container operating systems have progressed significantly, with fully

automated systems leading the way. For instance, the use of automated machines has helped container terminals become even more productive and more efficient with less labor. Much of the container stacking handlers used to stack the containers in the container yard are remote-controlled by an operator inside a terminal building. This eliminates many safety hazards on the terminal, increases the personal comfort level of the operator of the equipment handler, and gives the operator a better view of the terminal, as the container handler is normally fully equipped with multiple closed circuit television monitors.

More recently, some modern container terminals have fully automated vehicles/equipment handlers, which require no human interaction to operate, since they use GPS technology for navigation. These handlers constantly track each container and wirelessly transfer information to a main computer, where it is

Types of Terminal Operating Systems



The following is a list of terminal operators with their own terminal operating system:



Hutchinson Port Holdings (nGen)—Hong Kong

PSA International (Portnet)—Singapore

Ports America, Inc. (Ports America System)—Iselin, N.J.

TSI Terminal Systems, Inc. (TSI System)—Vancouver, BC, Canada

Maher Terminals LLC (Maher System)—Elizabeth, N.J.

stored and updated. The future of containerized terminal operating systems are very broad in scope but the trend is to fully integrate the entire supply chain for a customer and/or shipper.

There are many different systems with different providers along the supply chain, which can cause some issues. For example, many of the terminal's customers and vendors have different computer operating systems and need to send and retrieve information from the container terminal operator's main system.

To remedy this issue, a terminal operator can require customers and vendors to use the terminal's specific operating system; however, this may create problems for the customers and vendors, as well as for the terminal operator. More specifically, terminal's custom-

ers and vendors may be forced to purchase different systems for each container terminal they deal with.

Conversely, the container terminal could develop a "market-based system," in which the users of the supply chain are presented with goals and offer bids to meet those goals. Another option is to develop and implement a true Web-based system with access codes that will allow each user to retrieve information on a need-to-know basis.

Terminal operators have seen the importance of information technology. Operators will continue to use it to grow, as they have done in the past.

About the authors:

Captain Jeremy Sykes holds an M.S. in maritime and transport management from University of Antwerp, Belgium, an M.B.A. from Old Dominion University, and a B.A. from Virginia Wesleyan College. He also holds a current U.S.C.G. 100-Ton Inland Masters License. He is an account executive at MDP Marine Insurance and has worked as a ship agent, relief captain/mate, and a claims advocate.

Mr. Ed Merkle is the director of Port Security and Emergency Operations for the Virginia Port Authority. He also serves as an executive member of the area maritime security committee and is appointed to the national maritime security advisory council. He is a retired Coast Guard captain, with more than 25 years of active military service. He is a graduate of the U.S. Coast Guard Academy and holds an M.Ed. degree from George Washington University.

Bibliography:

- Barnard, Bruce, "Container Ship Charter Rates Fall 30 Percent," Journal of Commerce Online, December 9, 2010.
- Bushey, Steve, "Information Technology and Terminal Operations," AAPA & NAWA Marine Terminal Management Program at the AAPA 2008 Conference.
- Couper, A., "Social Consequences of Maritime Technological Change," Washington Sea Grant Program, Washington, 1985.
- Dally, H.K., "Systems Analysis—I: Study of Deep-sea Multi-User Berths," In: Containers—Their Handling and Transport: A Survey of Current Practice. Cargo Systems International, London, 1979.
- Henesey, Lawrence Edward, "Enhancing Container Terminal Performance: A Multi Agent Systems Approach," Blekinge Institute of Technology, Sweden, 2004.
- Kia, M., E. Shayan, and F. Ghotb, "The importance of information technology in port operations," International Journal of Physical Distribution & Logistics Management.
- Levinson, Mark, "The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger," Princeton: Princeton UP, 2006.
- Lui, Eric, and Mrs. Poh Hui Ying, "Computerized Container Terminal Management," No. 10. UNCTAD Monographs on Port Management.
- MARAD, Glossary of Shipping Terms.
- Navis, LLC, "Marine Terminal Operations Technology: Past, Present and Future," White paper.
- Thys, "Real-time Container Terminal," In: 7th Terminal Operations Conference, Genoa.

AIS in Action

*Enhancing maritime domain awareness
in America's waterways, ports, and terminals.*

by MR. JASON TIEMAN
*Director of Maritime Solutions
AIRSIS*

Maritime domain awareness is critical to U.S. interests and worldwide economic stability and growth. Increasingly, government agencies and other organizations are enhancing maritime domain awareness (MDA) programs by using Automatic Identification System (AIS) data to monitor and derive intelligence from information about real-time and historical vessel movements in major ports and waterways.

The Department of Defense Executive Agent for Maritime Domain Awareness (DoD EAMDA) has recognized AIS as a potential tool for enhancing MDA initiatives. In May 2010, the EAMDA announced plans to integrate capabilities that enable non-classified information sharing to build partnership capacities. The focus: Define an integration architecture that can be used for non-classified data sharing, and standardize the Virtual Regional Maritime Traffic Center suite, utilizing AIS data via an Internet-based system.

Integrating AIS into Safety, Security, and MDA Programs

There are many examples of how the Automatic Identification System helps ensure the safety and security of the maritime domain. For example, several major ports are using AIS data to monitor compliance with voluntary speed limits. One major southwestern U.S. port has established a program to reduce speeds to 12 knots for cargo ships and 15 knots for cruise ships inside the harbor and within a specified distance seaward. Port management uses web-based AIS vessel tracking to record the maximum speed of all vessels traveling in its vessel speed reduction zone. Port officials identify vessel operators who achieve 90 percent program compliance rate and recognizes them for their participation each quarter.¹

AIS can also be used to protect high-risk targets such as tankers, which are particularly vulnerable to security threats because they tend to move very large volumes of oil and gas through a small number of choke points. They are at greatest risk when entering or leaving port and when moored. Automatic Identification System information gives users a more complete picture of other traffic.






In the private domain, many marine terminal operators are also using AIS to assist with security programs. Today's systems enable them to define their own customized fleets of chartered vessels, workboats, tugs, and barges that they wish to monitor, and to receive and share email and text-message alerts about fleet movements. This also enables operators to automatically time-stamp and capture data about arrivals, departures, and other vessel events; add their own documents and information about dockside events for each vessel call; and quickly access historical data and animated playback for any selected vessels and events.

While some services use AIS data to create "points on a map," this is inadequate for comprehensive maritime security and other business initiatives. For this data to be a useful MDA tool, it must be possible to view, synthesize, analyze, and make decisions based on real-time and historical information about the activities of every AIS-enabled vessel in every region of interest. The ability to look at historical vessel movements is particularly important, since this information can be used to analyze the situation, modify maritime domain awareness initiatives, and identify best practices for pre-empting and/or mitigating threats.





How AIS Works

Since 2005, every commercial vessel that trades at a U.S. port and most international destinations has been required to transmit its ship identifier and location through standard AIS transponders. While the primary purpose originally was collision avoidance, it has increasingly been adopted for maritime security, general safety, and other business-intelligence applications. AIS data is used for these purposes by vessel traffic service operators, law enforcement agencies, the U.S. Coast Guard, major oil companies, and other large vessel owners and operators, as well as port and marine terminal management and many other maritime professionals.

Automatic Identification System transponders broadcast a variety of static and dynamic information on a fixed schedule that ranges from two to 10 seconds to six minutes. Static data includes:

-  the ship's name and call sign,
-  its unique International Maritime Organization or Maritime Mobile Service Identity number,
-  its beam and length,
-  the ship type,
-  its antenna location.

Dynamic data includes:

-  the time and the ship's current position,
-  course and speed over ground,
-  gyro heading and rate of turn,
-  navigational status.

AIS also broadcasts voyage-related data including the ship's draft, cargo information and destination, plus estimated time of arrival.

Bibliography:

www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx

AIS-based vessel-monitoring services also should have command-and-control display capabilities to streamline security program tasks, while simultaneously optimizing operational efficiency for operations like scheduling labor and other resources. Users are

able to filter results by ship and port or region, and create user-defined tracking-related zones to enhance vessel viewing, tracking, and alerts. This should allow users to focus on specific regions of concern, and to more closely monitor for specific, anomalous behavior that might indicate an emerging threat situation.

For even better visibility, small satellite tracking units can be used to acquire tracking information about unmanned barges, buoys, and other high-value assets, which can then be combined with AIS vessel data to give users a more complete picture of other traffic.

Leveraging AIS for Broader Business Applications

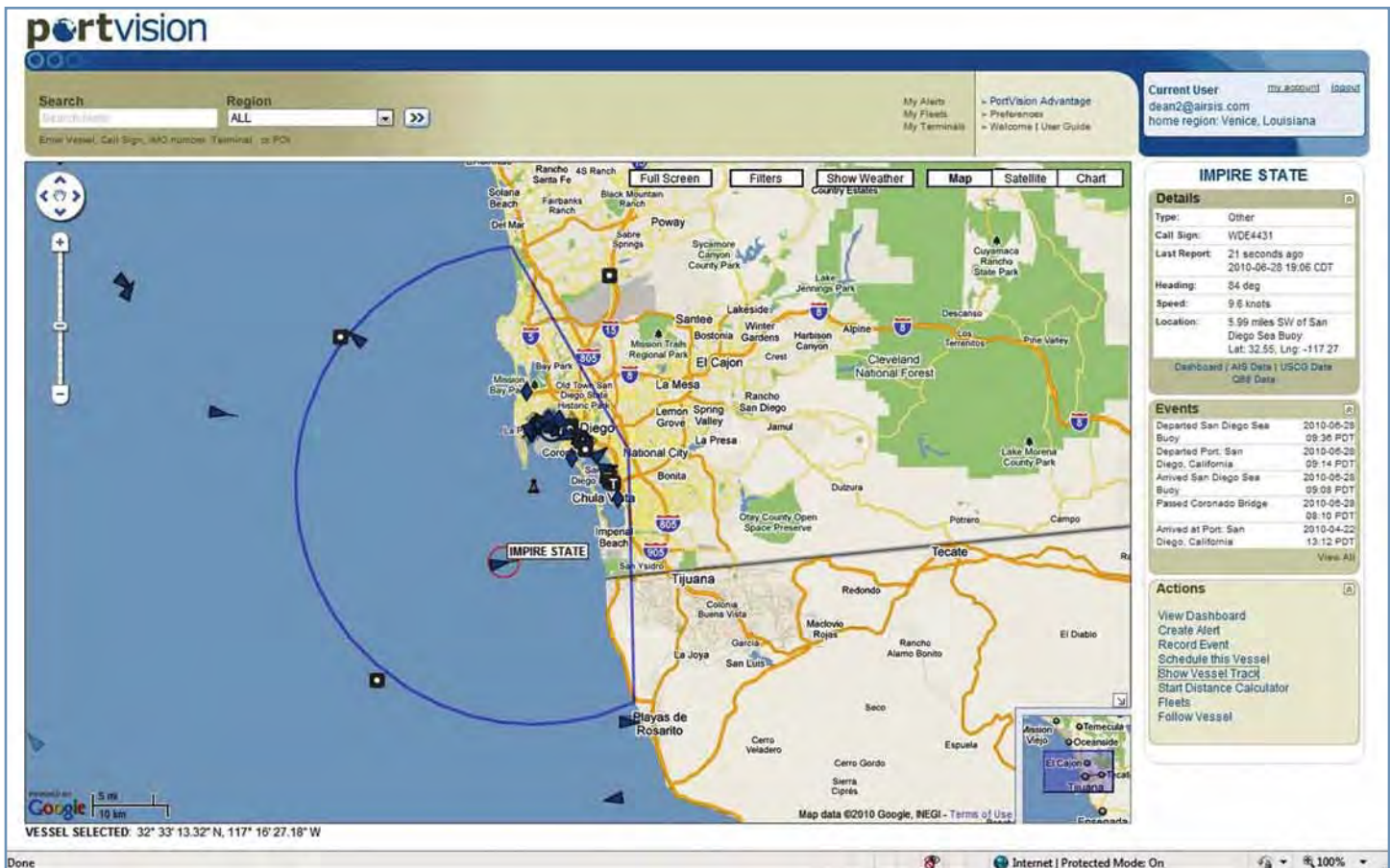
AIS-based vessel-tracking services are commonly used to enhance security and maritime domain awareness initiatives, but can also be used for a variety of business-intelligence purposes. For instance, vessel owners and terminal operators can perform integrated demurrage reporting and analysis, verify demurrage claims, and produce required documentation, all within a single, integrated dashboard environment.

Information on vessel transits can also provide better contract accountability related to speed, fuel consumption, and transit routes for vessels supporting drilling operations for offshore platforms. For refiners and terminals, AIS provides the convenience of knowing when a ship arrives at a sea buoy, the status of pilots or harbor tugs, and the location of a tow for tug and barge activity. This simplifies resource planning and enables just-in-time deployment based on current vessel locations, ETAs, dock availability, and in-transit traffic conditions.

Looking Ahead

Today's wealth of aggregated AIS information can also be used to generate competitive analyses of offshore fleets, validate vessel activities and costs, and improve market intelligence pertaining to tanker and barge availability.

To realize all these benefits, these systems must be easy to integrate into existing business systems and should incorporate other data, including real-time weather radar overlays and animated loops, plus voyage distance calculations and vessel arrival estimations. Finally, AIS systems should enable users to add documents and other information for each vessel call, such as cargo manifests or photographs of cargo.



AIS data provides a Web-based view of vessels traveling within an identified zone in a U.S port.

AIS-based ship tracking continues to grow beyond its original role, which was primarily to minimize collisions between commercial vessels. Today's AIS-based vessel-tracking services give users a real-time view of vessel traffic in a single command-and-control display environment focused on user-defined monitoring zones, and facilitates real-time information sharing and reporting with remote participants and other operation centers.

By combining real-time visualization and historical information with comprehensive management tools, the latest AIS-based vessel-tracking systems deliver extensive waterway mapping, alerting, reporting and

analysis capabilities, which can enhance maritime domain awareness and improve security initiatives.

About the author:

Mr. Tieman served seven years as a Coast Guard officer and continues to serve as a reserve Lieutenant Commander. He holds an unlimited tonnage third mate license and has served on tankers, supply vessels, research vessels, and harbor tugs. He has also been critical in the development and implementation of PortVision, a maritime software product of AIRSIS. He holds a B.S. in maritime transportation from Texas A&M Galveston and an M.S. in quality systems management.

Endnote:

¹. www.portofsandiego.org



APPROVED FOR TRANSPORT
UNDER CUSTOMS SEAL

TR / 50078

TYPE
NU 20-2001-T

MANUFACTURER'S SERIAL NO
MU 82-D- 01180

OWNED OR MANAGED BY
CRONOS CONTAINERS LTD.
UNITED KINGDOM

TIMBER COMPONENT TREATMENT
IM / CHLORDANE / 82

CSC SAFETY APPROVAL

F / BV / 4008 / 92

DATE MANUFACTURED

17 9 / 1992

IDENTIFICATION NO

USA 0484340

MAXIMUM GROSS MASS

24000 KG 52810 LBS

ALLOW. STACK. WT. FOR L&G

182000 KG 423280 LBS

LIFTING TEST LOAD VALUE

15240 KG 33600 LBS

MANUFACTURED BY

MED UNION CONTAINERS A.S.
12MIR / TORIKYE

IMDG
2013
INSPECTION
SHALL BE
BEFORE
THE
HORN
POUNDED
BY THE
YEAR
SIGNIFY
ON THIS
DECAL
CSC
NON-
IMDG

MIL DO4

U.S. Coast Guard photo
by LCDR Doug Lincoln.

Securing Certain Dangerous Cargoes

by MR. BOB REIMANN
Cargo Security
U.S. Coast Guard Headquarters

MR. MARK JOHNSON
Senior Vice President
C & H Global Security

The transit, transfer, and storage of certain dangerous cargoes (CDCs) along our nation's waterways present particular security challenges for those charged with ensuring no harm comes to adjacent populations and critical infrastructure. Such cargo has chemical characteristics that can result in significant health or infrastructure impact in an uncontrolled release.

As such, the Coast Guard identifies bulk CDC transits, transfers, and storage as one of the highest daily security risks on U.S. waterways and has embarked on a risk-based approach to CDC security. This strategic and tactical approach considers the reality of limited federal resources against the significant consequences of a successful terrorist to ultimately establish and manage an acceptable CDC security risk. Primary to this approach is developing a national certain dangerous cargoes security strategy and implementation plan that spans the security spectrum from awareness, prevention, and protection to response and recovery.

Security in Action

The national CDC security strategy focuses on intentional attacks to the portion of the U.S. marine transportation system (MTS) that supports bulk CDC vessel transits, vessel/facility transfers, and facility storage. It integrates the elements of the security spectrum with the elements of the risk equation (risk = threat × vulnerability × consequence) through operational and internal management goals.

Goals include:

AWARENESS: Provide real-time awareness of the risk of intentional attacks on CDCs to stakeholders. This is the principal driver for resource allocation decisions and envisions integrating maritime domain awareness input with risk modeling to facilitate captain of the port resource management and other operational decision making.

CDCs Defined

Certain dangerous cargoes are defined in 33 CFR 160.204 as products having chemical properties such as toxicity, flammability, and reactivity that, if released, could produce devastating consequences on surrounding cities/towns, and/or critical infrastructure and key resources.

While the regulation includes more commodities than the ones specifically noted below, the following are considered the most hazardous (generally when carried in bulk), and are the ones on which the Coast Guard currently focuses to reduce their vulnerability to attack:

anhydrous ammonia
ammonium nitrate
chlorine
liquefied natural gas
liquefied petroleum gas

Coast Guard CDC Security

The Coast Guard has been studying the CDC security issue since September of 2009, when it hosted, along with the National Maritime Security Advisory Committee, a cargo security symposium in Reston, Va. As a result, the Coast Guard chartered a more focused CDC risk reduction workgroup, including public and private stakeholder representatives. The workgroup met from December 2009 to October 2010, producing an internal report in April 2011. The chartered study areas, along with the symposium results, are informing development of the national CDC security strategy.

There is concern that one CDC (liquefied natural gas) has received attention to the detriment of other equally or more dangerous cargoes. That, and the scope of coverage necessary under current operational risk-reduction guidance, were the principal drivers to analyze how the Coast Guard manages CDC security and what might be done to tightly manage the risk of a CDC attack, which was the impetus for developing the national CDC security strategy. Coincident to this was the requirement in the Coast Guard's 2010/2011 Authorization Act to produce the same strategy and a study that describes current and planned actions.



Emergency evacuation drill. U.S. Coast Guard photo by Petty Officer Richard Brahm.



Atlantic Strike Team members participate in a Hazmat exercise. U.S. Coast Guard photo by CDR David Haynes.

PREVENTION AND PROTECTION: Assess MTS vulnerability to threats of intentional attacks on CDCs and mitigate the vulnerability to an acceptable level. This is the element of the risk equation over which the Coast Guard has the most control. This goal also forces the Coast Guard to define how much risk is acceptable to absorb locally, regionally and nationally and then manage to that security level, potentially blending the abstract with operational reality.

It further envisions dynamic preparedness assessment to blunt or absorb threats and models the assessment results against acceptable risk. This allows captains of the port to determine whether stakeholder measures are sufficient or if Coast Guard operational resources must be deployed to meet acceptable risk levels.

RESPONSE: Dynamically assess the potential consequences of intentional attacks and mitigate, through coordinated response, the impact of a successful attack. This goal focuses on the first part of the "consequence" element of the risk equation, allowing the sector commanders to assess USCG and

community response preparedness and appropriately allocate USCG resources.

RECOVERY: Develop national, regional, and local resiliency/recovery capability. Resiliency relies on various components within a community to return some acceptable level of functionality—economically and socially. Like the response goal, this focuses on CG readiness and asset allocation. However, recovery aspects are not as fully developed as response; thus the goal also encourages the Coast Guard to lead the effort to recover from a CDC security event through multi-stakeholder planning efforts.

INTERNAL MANAGEMENT: Establish internal organization and processes and stakeholder relationships to manage the national maritime CDC security program to an acceptable risk level. Organization, standards and policy promulgation, budget, and stakeholder agreements form the core of the goal's purpose. Key underlying components are the ability to measure CDC program progress and identifying an accountable program manager.

Objectives and Key Implementation Components

The national CDC security strategy will help policy makers and operational practitioners to understand the nature of the goals and how they are to be met. As such, each goal contains supporting objectives and each objective contains key implementation components that the national program manager can use in driving toward goal achievement.

From a practical standpoint, managing the objectives will be the program manager's primary goal-achievement method. This will be greatly aided by the strategy's companion document, the implementation plan, which will lay out in detail how objectives

will be met, over what timeline, including necessary resourcing, and responsible parties.

The Coast Guard will regularly review the strategy, focusing on measures of effectiveness, which will allow it to be a model for developing similar mission strategies.

Stakeholder Input

As part of the strategy development process, public listening sessions were held and stakeholder feedback incorporated in the draft national CDC strategy. Following in-house briefings, the strategy will be fully developed for submission to Congress and the nucleus for policy for that aspect of the USCG ports, waterways, and coastal security mission.

Security strategy lays out the charted course, but it takes a robust implementation plan to bring the strategy to life. The Coast Guard will draft the implementation plan that will describe in detail how CDC security risk will be managed on a daily basis.

About the authors:

Mr. Bob Reimann has more than 24 years of federal experience as a security specialist with the U.S. Navy and Coast Guard. He serves as the subject matter expert for issues regarding cargo security as related to the Coast Guard's Port Security and Homeland Security missions. Mr. Reimann develops agency-wide policy, initiatives, risk management tools, and procedures for implementation of cargo security activities within the Coast Guard. He holds a B.S. in business administration from Ferrum College.

Captain Mark H. Johnson is the senior vice president for C & H Global Security. He is a former deputy assistant administrator for maritime and land security of the Transportation Security Administration, and a former U.S. Coast Guard career officer specializing in safety, security, and environmental protection. Captain Johnson is also a former U.S. Coast Guard captain of the port. He received his B.S. from the U.S. Coast Guard Academy and his M.S. from the University of Southern California.

Multi-Agency Strike Force Operations

Combining forces extends capabilities.

by LCDR KEVIN LYNN
Cargo and Facilities Division
U.S. Coast Guard

What do smuggled narcotics, shipments of undeclared hazardous materials, secreted migrants, and illicit weapons and ammunition have in common? Certainly each presents a potentially serious violation of U.S. law, but each can also be found in the containerized cargo transport mode.

Responsible shippers dedicate great effort to ensuring their shipment is offered in compliance with U.S. laws and international codes, and many protect what can

be highly valuable shipments with locking security bolt seals. However, when the container is in transit, security safeguards can be overcome and illegal materials added to an otherwise legitimate shipment.

The U.S. Coast Guard has been performing container inspections since 1994, when the Department of Transportation and Related Agencies Appropriations Act provided funding for personnel to ensure shipments are in compliance with the Federal Hazardous Materials Transportation Law and the International Safe Container Act of 1977.

The national container inspection program is built on this foundation, and Coast Guard container inspectors have examined hundreds of thousands of containers.

But what about those situations described earlier? How can the Coast Guard contribute to finding and deterring illegal activities that lead to a more secure cargo supply chain? Part of the answer lies with the multi-agency strike force operation (MASFO).

Understanding the MASFO

A multi-agency strike force operation involves surging cargo container inspection enforcement activity by combining the efforts of multiple agencies with varying jurisdictions, authorities, and resources. The Coast Guard typically leads MASFOs as the agency with primary responsibility for waterfront facility operations. Such operations can range from a few hours involving two or three partner agencies, to several days

continued on page 54

Who's Involved?

Federal Agencies

U.S. Coast Guard
Customs and Border Protection
Federal Motor Carriers Safety Administration
Pipeline and Hazardous Materials Safety Administration
Federal Railroad Administration
Animal and Plant Health Inspection Service
Transportation Security Administration

State and Local Agencies

Port Authorities
State, Local, and Harbor Police
State Department of Transportation
Fire Departments/Hazardous Materials Unit

Non-Governmental Organizations

National Cargo Bureau

Petty Officer Angela Ford inspects a cargo container. MASFO inspections include verifying truck and container documentation; container structural integrity; customs and fuel tax compliance; and hazardous material markings, packaging, and segregation. U.S. Coast Guard photo by Petty Officer Brandyn Hill.



Petty Officer Brian Villeroel and Petty Officer Joshua Lockwood conduct a multi-agency strike force operation with CBP personnel and local police at Hampton Roads port facilities. U.S. Coast Guard photo by Lt. Ronaydee Marquez.



Personnel inspect trucks during a multi-agency strike force operation at the Maryland Port Administration's Seagirt Marine Terminal. U.S. Coast Guard photo by Petty Officer Brandyn Hill.





CBP Canine Enforcement Officer Patrick Roche lifts Sinbad, a narcotics detecting dog, into a cargo container during a multi-agency strike force operation. U.S. Coast Guard photo by Petty Officer Robert Brazzell.

in duration with numerous local, state, and federal agencies.

Coast Guard captain of the port units involved with the national container inspection program should coordinate multi-agency strike force operations at a frequency appropriate for the scale of container operations at the port facilities. Typically those units with ports handling in excess of 500,000 20-foot equivalent containers should conduct at least one multi-agency strike force operation per year, but any unit can conduct a MASFO.

One of the most important elements to consider is how well you know and work with the existing inter-agency partners who will become part of the team. A strong understanding of each agency's or organization's roles, authorities, and resources is absolutely necessary before operations begin.

MASFOs and Cargo Security

When considering the shared responsibilities of protecting life and property from subversive acts such as theft, sabotage, or terrorism, multi-agency strike force operations go a great distance in meeting homeland security objectives. During the course of a single MASFO, dozens to hundreds of containers

can be examined for signs of tampering or other non-compliance, such as missing or inconsistent security bolt seals, improper container documentation/markings, or other evidence that may raise suspicion. When such issues are raised during an operation, there is a higher likelihood that an agency having authority is immediately available to take appropriate action.

The benefit of deterrence can go unrecognized with security related operations. However, performing regular MASFOs can send a clear signal that security forces are proactive, cooperative, and efficient. To maintain this perception, properly concluding a multi-agency strike force operation can be just as important as planning for one. Additionally, to make the next MASFO even more successful, it's important to take the time to properly debrief participating agencies, document efforts and findings, and incorporate lessons learned and best practices. Without these crucial steps, a multi-agency strike force operation may never achieve its full potential or effectiveness.

Moving Ahead

The Coast Guard continues to press forward to conduct container inspections and MASFOs. During challenging times when budgets are constrained and resources stretched, these operations can effectively harness the collective talents of America's best security oriented forces. Together, the Coast Guard and other agencies can secure the cargo supply chain, port by port, and container by container.

About the author:

LCDR Kevin P. Lynn serves as chief, Facility Safety Branch, at U.S. Coast Guard headquarters. He graduated from the U.S. Coast Guard Academy with a B.S. in marine and environmental sciences. He also served at the Marine Safety Office in New Orleans, La., and at Marine Safety Unit Savannah, Ga., where he directed Coast Guard activities related to port security, defense readiness, environmental response, and waterways management.

For more INFORMATION:

The Coast Guard's Container Inspection Training and Assistance Team (CITAT) is a specialized force that deals solely with container inspections. In addition to local Coast Guard captain of the port resources, CITAT can assist Coast Guard units in establishing a MASFO program.

CITAT is based in Oklahoma City, Okla., and can be contacted by visiting

<http://homeport.uscg.mil>

and selecting "containers" from the left menu.

Los Angeles Port Police

*Using advanced technology
to reduce the risk of terrorism.*

by MR. GEORGE CUMMINGS, USCG RET.
*Director of Homeland Security and Support Services
Los Angeles Port Police*

The port police are part of the City of Los Angeles's Harbor Department. Since the terrorist attacks of September 11, 2001, port police have worked to reduce the risk of terrorist attack intended to impede port operations. Efforts are focused on advanced technology, continuous training, and interagency cooperation.

Maintaining a visible presence on land and water is a major deterrent to a terrorist act, so the port has added new patrol boats, additional police vehicles, and an increase in the overall compliment of sworn officers.

Threat Response

A terrorist takeover of a deep-draft vessel is one of the threats identified within the maritime environment.

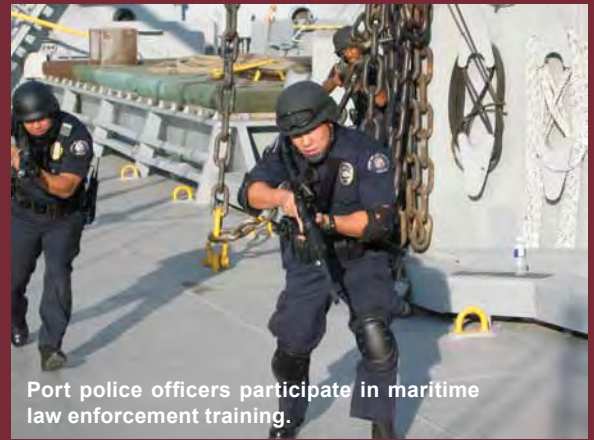


To counter this threat, joint agency teams of sea marshals were trained and deployed immediately after 9/11. The port police continue to perform this mission as a standard part of operations; armed officers board selected deep-draft vessels as they enter and depart the port.

The port police have also greatly enhanced diving and underwater detection capabilities to conduct security sweeps of piers and hull searches via underwater remotely-operated vehicles (ROVs). These ROVs are designed to enhance the safety and strengthen the community by aiding in the detection of underwater explosives and foreign objects. As a part of this duty, officers conduct channel bottom mapping surveys of the Los Angeles main channel and adjoining waterways within the port, which are compared to baseline surveys to detect changes. Divers then investigate anomalies.

The K-9 Unit

Officers and their trained dogs are deployed at the cruise terminal and the Catalina Island ferry terminal to detect explosives. Explosive detection dogs also accompany their handlers on various deep-draft vessel boardings.



Port police officers participate in maritime law enforcement training.

New Technology

LA's port officials have installed a highly sophisticated port-wide surveillance camera system, provided by the Federal Port Security Grant program. This system includes pan-tilt-zoom cameras as well

as high-power infrared units, and is equipped with analytics that allow watchstanders to set virtual perimeters around critical assets within the port. The system alerts watchstanders if anything crosses its virtual perimeter.

Port security grant funding was also used to purchase a situational awareness system that integrates input feeds from several different sensor systems and provides a single display at the watchstander's station



Port police patrol boat underway in the main channel.

Central California Area Maritime Security Committee

The Central California Area Maritime Security Committee was established in 2004 as a result of the Maritime Transportation Security Act. The committee is chaired by the U.S. Coast Guard sector commander and membership includes all of the federal, state, local law enforcement, and emergency response agencies that operate within the Port of Los Angeles and the Port of Long Beach.

Additionally, committee membership includes representatives of the marine exchange, the port terminals, elected officials, and the longshore labor union. Subcommittees focus on operational and logistical planning, training and exercises, intelligence sharing, and port stakeholder issues like distributing port security grant funds.

The port police also employ a high-energy, mobile x-ray scanning unit that provides detailed images of the cargo carried by commercial vehicles. It is used primarily at the Los Angeles cruise terminal to examine delivery trucks and other vehicles.

Training

The Port of Los Angeles, in partnership with the State of California Emergency Management Agency, and the U.S. Department of Homeland Security, has developed the country's first maritime law enforcement training course. This five-week course focuses on instruction for crewmembers on law enforcement vessels developed jointly by the Los Angeles County Sheriff's Department, Los Angeles Port Police, and Long Beach Police Department. The course is California Police Officer Standards and Training certified and consistent with current federal doctrine.

with site-specific information, pictures, building or utility plans, and drawings. The system can link remotely to mobile units in patrol cars, police boats, and handheld units.

One of the critical operational concerns identified following the terrorist attacks of 9/11 was the need for radio communications among multiple responding agencies. To address this need, port police added an interoperable radio console to their dispatch radio system, which allows them to rapidly patch different radio channels together so units from different agencies can communicate during joint agency response operations. Additionally, a mobile communications vehicle can be deployed as part of a multi-agency incident response.

Going forward, the Los Angeles port police will continue to compile best practices, encourage interagency cooperation, and evaluate new technology to improve their effectiveness as they conduct port security operations.

About the author:

Mr. George Cummings retired from the U.S. Coast Guard as a commander after serving as a commissioned officer for 21 years. His career included shipboard engineering, marine safety, and maritime security assignments. His final assignment was alternate captain of the port and deputy group commander, MSO/Group Los Angeles-Long Beach. His formal education includes a B.A. in marine engineering from the U.S. Coast Guard Academy, and an M.A. in mechanical engineering from the U.S. Naval Post Graduate School.

Area Maritime Security Plans

Securing the global supply chain.

by MR. MICHAEL P. SMITH
U.S. Coast Guard

Office of Counterterrorism and Defense Operations

Maintaining preparedness to secure the global supply chain requires a significant and varied amount of planning, especially at the domestic maritime port level. Within the area maritime security (AMS) preparedness program, Coast Guard planners work AMS plans with area maritime security committees and other maritime stakeholders to help secure the U.S. marine transportation system (MTS) portion of the global supply chain through continual improvements to strategic, operational, and tactical planning.

The terrorist attacks of Sept. 11, 2001, sparked a new awareness of potential risks to the U.S. marine transportation system, which in turn has substantially changed planning approaches. As the MTS is a critical resource, the Coast Guard also re-evaluated and strengthened its abilities to gauge the risk and protect the MTS and other critical infrastructure and key resources from possible terrorist attack.

The Coast Guard concentrates on five lines of focus: prevention, protection, response, initial recovery, and related logistics. Each has its own unique subject matter needs, contingency planning assumptions, training and exercise requirements. Remember, port-level preparedness is most effective well before an incident occurs.

History

On Nov. 25, 2002, the president signed the Maritime Transportation Security Act (MTSA) of 2002, which mandated developing area maritime security plans that are Coast Guard-coordinated efforts to prepare for and respond to transportation security incidents.

Coast Guard captains of the port serve as the federal maritime security coordinator (FMSC) for each of these area plans. As such, FMSCs establish and maintain area maritime security committees and consult with the members on matters pertaining to port security.

Guidance and Exercises

The Coast Guard provides a common template for area maritime security plans and guidance regarding developing and maintaining area maritime security committees—as well as guidance on conducting AMS assessments—within Navigation and Vessel Inspection Circular (NVIC) No. 9-02. The NVIC also addresses fulfilling MTSA requirements, and applies post-Katrina lessons learned relative to marine transportation system recovery. New additions to the NVIC include much expanded guidance to facilitate MTS recovery via a recovery plan template, and information on developing a salvage response plan, which is now required as an annex to each area maritime security plan.

To maintain and test effectiveness, AMS plans are exercised on a regular basis through the Coast Guard's Area Maritime Security Training and Exercise Program or AMSTEP. These interagency, multijurisdictional exercises encourage important interaction among port stakeholders and enable effective cooperation and preparation for contingencies and help identify and resolve gaps in planning, resources, and policy. After each exercise, after action reports evaluate lessons learned to identify shortfalls and implement appropriate corrective actions as needed.



Exercise Rescue Uncle Sam. U.S. Coast Guard members assist a “victim” aboard the tour boat *Uncle Sam* during a National Area Maritime Security Training Exercise Program event. USCG photo by Petty Officer Bill Colclough.

This interaction among federal, state, local, and tribal governments; local industry partners; and community representatives builds professional relationships and networks, while maximizing effective use of limited resources. Exercises can also help identify training requirements, an ongoing evolution that must exist in all stages of the preparedness process.

The Benefits

Area maritime security plans also serve to coordinate joint deterrence measures within the community. They provide linkages to emergency response plans and associated organizations, and they also serve as antiterrorism supporting plans to these tactical response activities during incident management. FMSCs and area maritime security committees contribute to the maritime common operating picture that permits critical decision makers to have access to

vital information. AMS plans support this effort, as they represent coordinated planning as a joint venture among many departments of the government and the civilian community at the port level.

Area maritime security committees and plans are successful cornerstones that bolster the lines of defense in our nation’s ports. Such collaborative planning, coordination, open lines of communication, working relationships, and unity of effort are essential to providing layered security and effective measures across all segments of the marine transportation system.

About the author:

Mr. Smith is a retired U.S. Navy captain working for the U.S. Coast Guard since 2003. He has served in many capacities including Navy special operations, U.S. Coast Guard port security assessments, and within the U.S. Coast Guard Area Maritime Security Training and Exercise Program.

Revolutionizing MTS Recovery

The Common Assessment and Reporting Tool.

by LTJG BRADLEY PATRICK BERGAN
U.S. Coast Guard
Office of Port and Facility Activities

Just the Facts

CART can automatically generate executive summaries, drawing from data within a particular CART event. These reports are exportable in portable document format or hypertext markup language and can be manually tailored to specific audiences such as senior leadership, industry, general public, and media.

The application can also produce localized reports for districts, sectors, MSUs, or associated captain of the port zones.

The Common Assessment and Reporting Tool (CART) is a prototype U.S. Coast Guard information technology system used to document, monitor, and report marine transportation system (MTS) status. CART is primarily an incident-recovery tool and is often used following a waterway threat or natural disaster. The tool provides near real-time MTS information throughout the Coast Guard chain of command; to other federal, state, and local government representatives; and to national, regional, and local level industry stakeholders.

Many Coast Guard commands have begun utilizing baseline information in CART to monitor the status of their command's local MTS on a daily basis, in addition to using information as part of a common operating picture during incidents and exercises.

System Contents and Capabilities

The Common Assessment and Reporting Tool contains EEI (essential elements of information) subsets that are divided into categories including:

- waterways and navigation systems,
- port area critical infrastructure,
- port area vessels,
- offshore energy,
- monitoring systems.

These elements are maintained as baseline or pre-incident information, and added to events as necessary following a significant marine transportation

continued on page 62

EI categories and subsets.



MTSR
Marine Transportation System Recovery



CART
Common Assessment and Reporting Tool

Waterways and Navigation Systems

- Aids to Navigation
- Deep Draft Channels
- Non-Deep Draft Channels
- Locks
- Vessel Salvage/Wreck Removal
- Oil Pollution Incidents
- Hazardous Materials Incidents

Port Area - Critical Infrastructure

- Bridges
- Bulk Liquid Facilities
- Container Cargo Facilities
- Non-containerized Cargo Facilities
- Shipyards
- High Capacity Passenger /Ferry Terminals

Port Area - Vessels

- Commercial Fishing Vessels
- High Capacity Passenger Vessels/Ferries
- Small Passenger Vessels
- Gaming Vessels
- Barge Traffic
- Barge Fleeting Areas

Offshore Energy

- Offshore Platforms
- Offshore Platforms (Top 100)
- Offshore Production
- Offshore Renewable Energy Installations (wind, wave, tidal)
- Mobile Offshore Drilling Units

Monitoring Systems

- Monitoring Systems (VTS, AIS)



U.S. COAST GUARD

Aids to Navigation	Miami Main Channel Lighted Buoy 11 (Jetty)	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Off Station. (Not available)
Aids to Navigation	Miami Main Channel Lighted Buoy 4 (Turn)	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Off Station. (Not available)
Aids to Navigation	Miami Main Channel Lighted Buoy 7 (Turn)	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Off Station. (Not available)
Deep Draft Channel	Government Cut	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Channel is blocked by the M/V El Rama. (Not available)
Bridges	SW 2nd Avenue Bridge	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Bridge is in the down position and appears heavily damaged and repair crew scene. (Not available)
Container Facilities	Container Facilities (POM)	<input type="radio"/> FA <input checked="" type="radio"/> PA <input type="radio"/> N/A	One crane has collapsed and is partially submerged in the water. There are numerous containers scattered throughout the port and in the water. Contents unknown. (Partially Available)
Bridges	NW 17th Avenue Bridge	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Bridge is stuck in down position. (Not available)
Bridges	Brickell Avenue Bridge	<input type="radio"/> FA <input type="radio"/> PA <input checked="" type="radio"/> N/A	Bridge has structural damage from a vessel collision. (Not available)

The status page delineates availability.

Report summaries identify vessels in queue, actions, and future plans.

Vessels in Queue 9/23/2008

Vessel queues offshore have returned to normal levels. the only remaining queues are associated with the inland barge traffic which is awaiting the opening of the GMW in the vicinity of Bolivar Roads. Effective at 6:00 A. M. Wednesday, September 24, 2008, the Gulf Intracoastal Waterway will be closed to westbound traffic at West Port Arthur bridge, mile 290, for a period of approximately 24 hours. This closure is necessary to clear the over 75 inland barge tows that are presently staged in the Intracoastal Waterway from mile 290 to mile 319 and the large backlog of eastbound traffic that is waiting to come to Port Arthur from Houston.

Waterways Management Actions 9/24/2008

Gulf Coast Joint Hurricane Team Protocols for USACE Galveston District are engaged with JHT teleconferences daily. NEW ORLEANS: The Morgan City/Port Allen Alternate Route open with restrictions at Bayou Sorrel Lock due to allision of bridge structure which is co-located at the lock facility. Bridge will open on signal from 2000 until 0600 daily.

Future Plans 9/23/2008

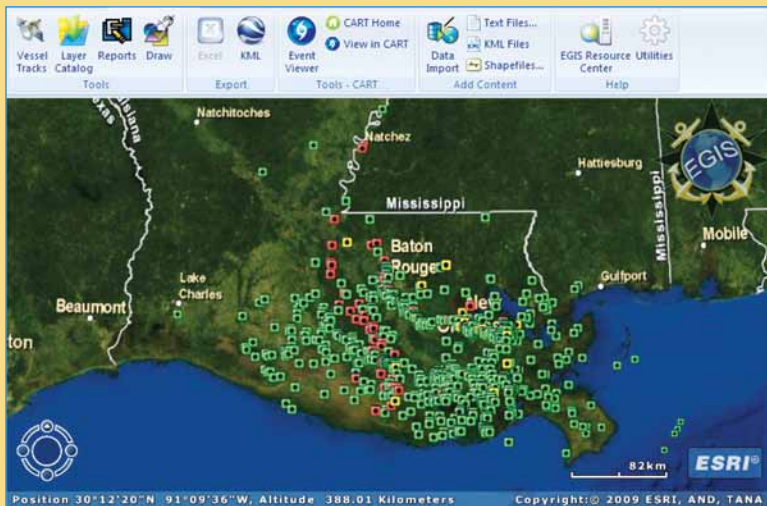
ATON RESTORATION PLANS USCG AtoN restoration continues. Although Cutters and ANTs are fully engaged in restoration efforts. The Houston-Galveston AOR remains a top priority, and efforts will be focused there. CGC JOSHUA APPEBY (D7) was released 22 Sep. SAGINAW and PAMLICO are completing range rebuilds in the Sabine-Neches waterway, once completed in a few days the nighttime restrictions on the waterway will be lifted. FACILITY DAMAGE ASSESSMENTS Facility assessments continue with emphasis on Port Arthur, Houston Ship Channel, Freeport and Texas City areas. Port Coordination Teams are coordinating efforts with CG facility inspectors to prioritize facility inspections and deep draft vessel movements consistent with terminal operating capabilities.

Port status identifies readiness/recovery status and individual port details.

Port and Status	Modified	Detail
BILOXI: Recovery - Open	9/13/2010	13SEP10(pm) Biloxi Back Bay and River. This small port will remain open to vessel traffic unless there is a threat of oil.
CHARLESTON: Recovery - Open	6/14/2010	The Port of Charleston remains open with no restrictions. All facilities operational as normal. No reported sightings of oil/sheen within the port.
GULFPORT: Recovery - Open	9/13/2010	13SEP10(pm) No changes. The Port of Gulfport remains open to all marine traffic with no restrictions. Gulfport vessel movement is estimated at 4 deep draft vessels per week.
JACKSONVILLE: Recovery - Open	5/24/2010	The Port of Jacksonville remains open with no restrictions. All facilities operational as normal. No reported sightings of oil/sheen within the port.
KEY WEST: Recovery - Open	5/19/2010	The Port of Key West remains open with no restrictions. All facilities operational as normal. No reported sightings of oil/sheen within the port. COTP Key West issued MSB applicable to arriving vessels transiting from areas affected by the oil spill.
MIAMI: Recovery - Open	8/2/2010	The Port of Miami remains open with no restrictions. All facilities operational as normal. No reported sightings of oil/sheen within the port. COTP Miami issued MSB applicable to arriving vessels transiting from areas affected by the oil spill. National Response Corp. notified COTP that OSRV Liberty and its response equipment will be temporarily out of the AOR in support of the Deepwater Horizon response efforts.
MOBILE: Recovery - Open	9/13/2010	13SEP10(pm) No changes. The Port of Mobile remains open to all traffic with no restrictions.



EGIS geospatial display shows CART event status:
 green—fully available;
 yellow—partially available;
 red—not available.



system disruption. “Events” can be created at the local, district, or area levels, and tailored to include specific units.

Within each Common Assessment and Reporting Tool event, there are tabs that include:

- event summary,
- event status,
- report summaries,
- port status.

The **event summary** section provides a table that auto-populates user data and captures the number of EEI instances and the status for each. There is also a text box for comments within this summary.

The **event status** section is where the status of individual EEIs can be characterized in one of three categories—fully available (FA), partially available (PA), and not available (NA). EEI availability is recorded in each EEI status text box. Entries in this section can relate to discrepancies with aids to navigation, bridges, or any of the other numerous EEIs captured within the Common Assessment and Reporting Tool.

The **report summaries** section contains information categories that can be added to an event to capture multiple perspectives and MTS components, including:

- port/incident area summary,
- MTS impact summary,
- MTS recovery actions summary,
- waterways management actions,
- vessels in queue,
- future plans.

Within the **port status** section, users can record port-specific data for each port in a captain of the port zone. In tracking port statuses, CART users can select from port readiness (pre-incident) or recovery conditions (post incident) as appropriate.

Future CART Development

To reduce redundant information gathering and documentation, a long-term goal is to interface with other Coast Guard systems, similar to the interface with Coast Guard Enterprise Geographic Information System.

Since its inception in 2008, users within the Common Assessment and Reporting Tool have created approximately 200 events, including incidents, drills, or exercises, and more than 900 registered users have accessed the system.

About the author:

LTJG Bradley Bergan administers the National Marine Transportation System Recovery Unit and serves as a Common Assessment and Reporting Tool project officer, Certain Dangerous Cargo assistant policy development project officer, and Freedom of Information Act officer. He has also served as a port state control officer and marine inspector. He is a graduate of Spring Hill College in Mobile, Ala.

Trade Recovery Protocols

Making the supply chain more resilient.

by MR. RYAN F. OWENS
Chief of Industry Outreach Branch
United States Coast Guard

The global supply chain system must be able to quickly recover from major disruptions, since this system is essential to the global economy, which in turn is essential to global peace and prosperity.

Building this systemic resilience requires deliberate efforts to minimize the aggregate impact of future events. In the face of inevitable disruptions, two of the most important aspects of resilience are systemic elasticity and the ability to surge and flex assets and resources.

Resilience also means ensuring adequate procedures for resuming post-incident trade, including measures to restore public confidence in system safety. This relies heavily upon assessments of critical infrastructure and key resource status, clear and open communications among all relevant partners, and collaboration with and adherence to prioritized cargo movement. It also requires active collaboration with sector stakeholders to:

- ◆ rapidly evaluate any impact on system capacity;
- ◆ prioritize the sequence for infrastructure regeneration;
- ◆ identify, obtain, and deploy supplies and personnel to maintain or increase capacity;
- ◆ re-establish cargo flow.

Maritime Recovery and Restoration Task Force

The Coast Guard formed the Maritime Recovery and Restoration Task Force (MR2TF) in the aftermath of Hurricane Katrina to ensure the service was aware of and specifically focused on issues impacting marine transportation system (MTS) recovery and restoration. The MR2TF focuses on port reconstitution, identifying regional and national issues, and coordinating

interagency and industry communication and problem resolution.

The task force also provides recommendations for better managing MTS recovery and restoration for future maritime incidents, including developing tools to assist decision makers during an MTS recovery event. As a result, Customs and Border Protection (CBP) and the Coast Guard signed the Joint Protocols for the Expeditious Recovery of Trade in 2006.

Joint Protocols for the Expeditious Recovery of Trade

Since no single government agency or private sector organization possesses the responsibility, the resources required, or the awareness needed to manage marine transportation system recovery following a maritime incident, the protocols establish a process for the collaborative recovery of maritime trade.

The protocols then aid maximum preparedness and a coordinated response to significant disruptions of the maritime trade system, to ensure government and private sector actions are coordinated or informed to most effectively and efficiently recover from such incidents.

The goals of these protocols:

- ◆ establish a communications process at the national level following or prior to an event causing a major disruption to the marine transportation system;
- ◆ consider the impact of a major MTS disruption to international commerce;
- ◆ support federal decision-making and protect federal interests;

Incident Communication

To assist implementation, the Coast Guard and CBP developed two groups:

1 the carrier support group leverages the major waterborne carriers' associations to understand macro-level maritime trade disruption,

2 the trade support group leverages other major domestic trade associations (rail and highway carriers, port authorities, etc.) that would be affected by major maritime trade system impact.

Additionally, the Coast Guard and CBP recognize that labor groups also play a critical role in the maritime and supply chain community and are exploring the feasibility of adding a labor support group.

Initiating the Protocols

The protocols may be triggered by actual or potential events including all hazards, such as natural disasters, transportation security incidents, major maritime incidents, declarations of incidents of national significance, or other circumstances significantly affecting the MTS.

Carrier Support Group

Cruise Line Industry Association
Passenger Vessel Association
Lake Carriers' Association
INTERTANKO
Chamber of Shipping
World Shipping Council
American Waterway Operators
BIMCO
INTERCARGO

Trade Support Group

American Association Port Authorities
Association of Inland Rivers, Ports & Terminals
National Association of Waterfront Employers
American Trucking Association
Association of American Railroads
U.S. Chamber of Commerce
American Association of Exporters & Importers
The Business Roundtable
Retail Industry Leaders Association
National Custom Brokers and Forwarders Association
National Industrial Transportation League
American Society of Transportation Logistics

Following initiation, the Coast Guard and CBP personnel conduct a conference call with the carrier and trade support groups to provide a situational update on the incident and communicate any MTS restrictions. Additionally, support group members are asked to provide any additional information regarding the industry response.

The support groups are then asked to act as information conduits to their constituents. Generally speaking, this initial communication will kick off a regular pattern of conference calls geared toward updating situation reports and eliciting feedback from the support group regarding business continuity intentions/plans until the recovery efforts are complete.

After the initial support group call, the Coast Guard and CBP will reach out to government partners to disseminate information about the critical incident and elicit input on MTS constraints. Then the Coast Guard and CBP develop national recommendations to facilitate trade resumption.

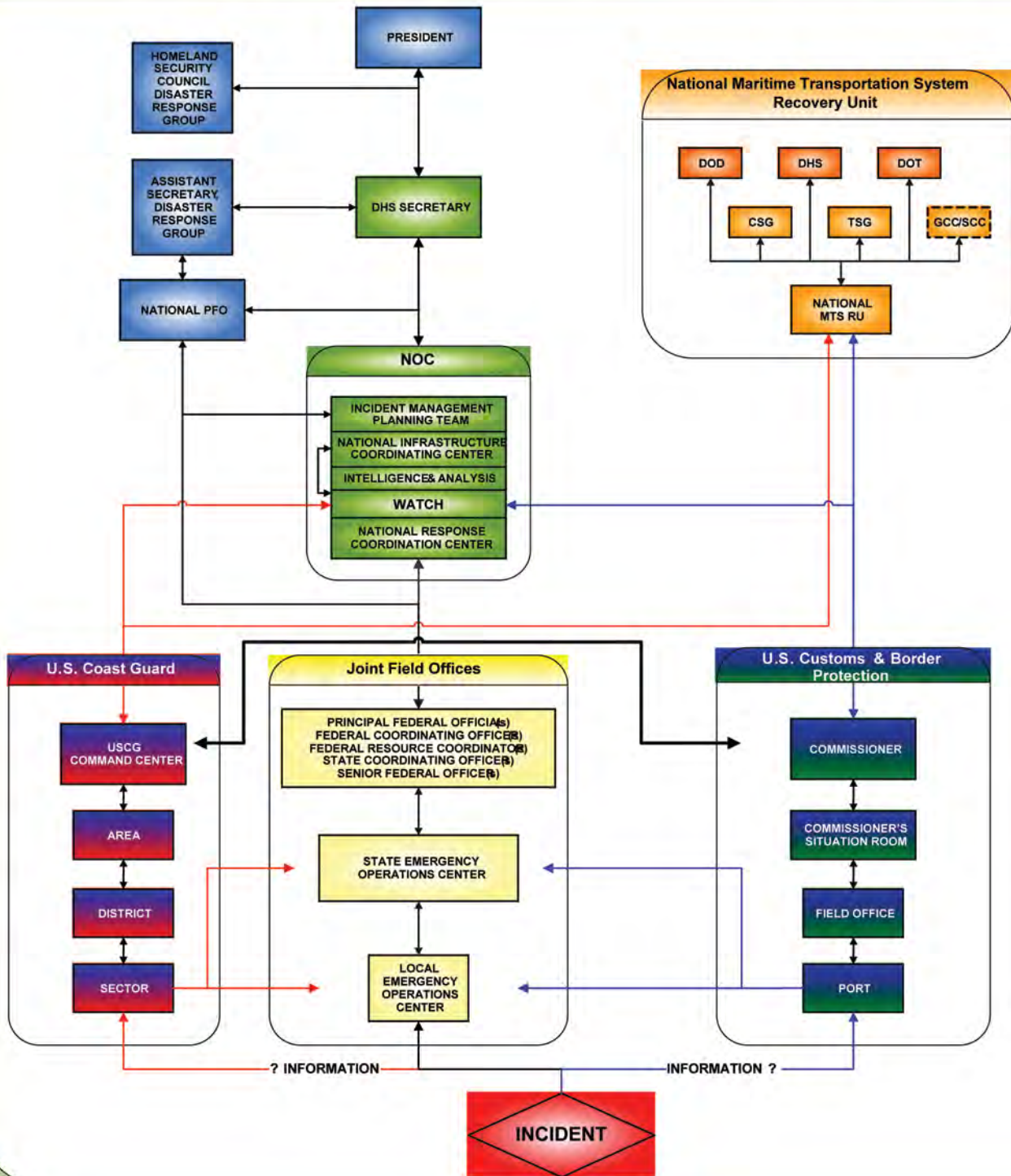
- ◆ establish how the Coast Guard and CBP will interact with other governmental agencies to facilitate the expeditious recovery of the national MTS and resumption of commerce, including maritime infrastructure recovery plan-related activities;
- ◆ support National Security Presidential Directive-41/Homeland Security Presidential Directive-13 and protect the national economy and national defense;

- ◆ support the SAFE Port Act of 2006 mandate to develop protocols for trade resumption.

As a significant disruption would include constraints on the system, effective communications and collaborative management within the reduced system

continued on page 66

U.S. CUSTOMS & BORDER PROTECTION / U.S. COAST GUARD INCIDENT COMMUNICATIONS FLOW CHART



capacity are critical to ensuring effective maritime commerce. To that end, the protocols:

- ◆ provide a forum for joint intergovernmental and joint government/private sector dialogues to identify and act on important issues to facilitate rapid maritime trade system recovery;
- ◆ assist senior-level decision makers by providing a process to collect and disseminate data on the status of the maritime trade system;
- ◆ assist senior-level decision makers by providing recommendations for national-level priorities or strategic actions necessary to facilitate rapid MTS recovery;
- ◆ help achieve balance among maritime transportation capability recovery and port, waterway, and cargo safety and security;
- ◆ provide for unified effort within the maritime community to maximize use of constrained transportation systems in support of the continuity or coordination of trade flow.

Essential Elements of Information

The protocols are not designed to make operational mission assignments, operational decisions, business decisions, or establish local or regional priorities. Further, developing a single set of actions is not practical, since every incident is different. The protocols describe general processes and activities that the federal government and industry members follow to ensure continuity of operations.

Generally speaking, the guidelines promote a framework of mutual collaboration between government and industry by sharing essential elements of infor-

mation, which are broken down into general categories including:

- ◆ waterways and navigation systems (aids to navigation, deep-draft channels, locks and dams);
- ◆ port area critical infrastructure (bridges, bulk liquid facilities, container cargo facilities);
- ◆ port area vessels;
- ◆ offshore energy;
- ◆ monitoring systems.

Communications and coordination are essential to reduce the impact of disruptions by better absorbing disruptions and being able to move resources and assess where they are needed in a timely matter. As such, a key component to the protocols is coordination among federal agencies and key industry support groups that act as communications links to the larger maritime and supply chain community. As such, these groups provide real-time information and feedback regarding their particular industry segment or set of constituents.

Protocols are used in coordinating trade continuity during incidents such as hurricanes, potential influenza outbreaks, or environmental incidents. During various responses, the U.S. enacted its protocols to successfully link national-level agencies with the private sector, to share vital information and develop a collaborative response.

About the author:

Mr. Ryan Owens is the chief of the Industry Outreach Branch in the U.S. Coast Guard's Domestic Ports Division. He is also the deputy designated federal official of the National Maritime Security Advisory Committee. He graduated as a licensed deck officer from Maine Maritime Academy and has served on a wide range of vessels, from container ships to oil rig supply ships.

Protecting the Supply Chain

The marine transportation system recovery unit.

by CDR CARLOS A. TORRES
 Chief, Domestic Ports Division
 U.S. Coast Guard Office of Port and Facility Activities

Marine Transportation System Components

The U.S. Marine Transportation System (MTS) is an integral part of the global supply chain. It provides passenger transportation by ferry, water taxi, and cruise ship, while supporting the economy, national security objectives and recreational activities. The MTS also includes vessels, vehicles, system users, harbors, waterways, ports, and their intermodal connections.

The harbors and waterways component of the marine transportation system is primarily managed and regulated by the U.S. Army Corp of Engineers (USACE) and the U.S. Coast Guard (USCG). If an incident impacts navigational channels, it is of the utmost importance that USACE quickly survey harbors and waterways to identify potential obstructions that might limit or impede ship transit. The USCG ensures that necessary aids to navigation are in place to facilitate reopening the navigational waterway.

Port terminals and associated marine facilities consist of buildings and slips where ships dock. More than 2,000 major port terminals exist in the U.S. Some are privately owned/operated facilities, while others are owned and operated by state government. The port terminal serves as an exchange site where cargo is disembarked from the ships and transferred to alternate means of transportation. The MTS is impacted if an incident prevents cargo flow. For example, cargo may not be able to be offloaded from the vessel, or moved from the facility if trucks or rail cars cannot access the pier's loading/unloading site.

Commercial ships are regulated by the USCG under strict inspection programs. However, factors such

human error, equipment failure, accidents, and heavy weather can disrupt ship operation, which can lead to the inability of this component to do its job—moving cargo.

Intermodal connections are hubs of transportation that include rail facilities, roads, and pipelines within or adjacent to the marine terminal. This is arguably the most complex and least understood component of the system. Post-incident recovery of the MTS needs to necessarily consider how the cargo is going to depart the seaport, since opening the harbors and waterways to receive cargo shipping would not achieve much if the roads and rail systems that move the cargo away from the port are not functional.

Therefore, from a recovery standpoint, it is important that all components of the MTS are understood. Whether an incident impacts only one of the components, or the whole system, an effective recovery isn't accomplished until all components are back in service.

Tracking MTS Recovery

Any marine transportation system interruption can have very serious implications for the economy, the security, and the overall welfare of the nation. Not surprisingly, the longer the disruption, the greater the potential impact. So, when the MTS becomes impacted, the main national effort focuses on returning it to normal as soon as possible.

For example, during the emergency responses that followed Hurricanes Katrina and Rita; a lot of attention was rightfully given to identifying marine transportation system damage and developing recovery

tactics. However, at that time, there was no existing protocol that could effectively track the marine transportation system recovery. The USCG subsequently directed all its field commands or sectors to develop an MTS baseline for their respective areas of responsibility, and to more effectively track post-incident recovery efforts by placing an MTS recovery unit (MTRU) within the existing local incident command system response organization.

A famous aphorism associated with operational management asserts that “what gets measured gets done.” In alignment with that concept, any effective marine transportation system recovery process must include measurable elements, including indicators that establish the current situation, how far the recovery process has to travel, and a clear idea of the desired end state.

With key measures in place, recovery operations can focus on certain desired outcomes as well as target areas or activities to achieve a specific goal and expedite the recovery. Since the desired state is pre-incident normalcy, the “normal” condition of the MTS has to be clearly understood and defined.

Creating an MTS Recovery Unit

To effectively evaluate the condition of a disrupted marine transportation system, the USCG constructed a baseline that quantifies the operational levels of the local MTS infrastructure, including essential ele-

ments of information (EEI) that reflect normal pre-incident levels of operations on specific areas of the MTS infrastructure.

MTS recovery units then track and report on the status of the recovery and restoration, and identify issues to facilitate the recovery process. To ensure similarity across the nation, the USCG mandated that the MTRU be placed within the planning section of the incident command system response organization for every incident that significantly impacts the marine transportation system. As such, the MTRU works side-by-side with the resources, situation, documentation, and demobilization units.

Additionally, MTS recovery units interact with maritime industry representatives as well as other government agencies that have mission responsibility over the different elements of the marine transportation system. Interaction with other stakeholders and members of the maritime community enhances MTRU effectiveness during operational responses.

As USCG sectors have stood up in a resource-constrained environment, the Coast Guard has been challenged to allocate the right type of talent and expertise to the MTS recovery unit without weakening other areas of the incident response organizations. The answer has been to incorporate maritime industry partnerships to assist in staffing MTS recovery units.



RDML Roy Nash, then deputy director of the National Maritime Intelligence Center, receives an on scene briefing from LCDR Mark Gibbs regarding port recovery efforts in Port au Prince, Haiti. U.S. Coast Guard photo by Petty Officer Eric J. Chandler.

About the author:

CDR Torres has served in the Coast Guard for 29 years, primarily in marine safety and prevention operations. He is a graduate of the University of Puerto Rico and has an M.A. in homeland security from American Military University.

Bibliography:

“The Marine Transportation System and the Federal Role: Measuring Performance, Targeting Improvement,” Transportation Research Board, 2004.

“National Dredging Needs Study of U.S. Ports and Harbors: Update 2000,” United States Army Corps of Engineers, 2003.

“Marine Transportation System Recovery,” Atlantic Area Instruction 16001.1, United States Coast Guard, 2006.

Trade Recovery

A complement to risk management.

by Ms. LOURITHA GREEN
Ian Axford Fellow

Risk management can prevent nefarious activities, but it cannot stop earthquakes or hurricanes, nor prevent every man-made incident. Therefore, countries use trade recovery protocols to respond to an incident and the resulting impact it has on trade. These plans focus on facilitating the movement of goods and people after a disruption.

Managing trade recovery requires:

- an accurate understanding of the disruption's cause;
- a clear, current assessment of the capacity of the affected transportation system(s);
- the ability to identify what goods are necessary to respond to the incident;
- effective communication with those responsible for the movement of goods, people, and conveyances;
- facilitation of that movement.

Customs administrations may hold responsibility for some or all trade recovery functions since movements often require crossing borders. In the United States, the responsibility for trade recovery is primarily shared between U.S. Customs and Border Protection (CBP) and the U.S. Coast Guard (USCG).

Developing Protocols

Governments cannot simply focus on the area that the incident directly impacts; therefore, the U.S. has taken a holistic view in developing certain protocols. For example, if an incident limits a port's ability to operate, other ports may have to process cargo that was to arrive at the initially affected area.

The U.S. has identified factors for efficient management of a disruption to prepare for this kind of challenge. They are:

- identifying transportation system capacities and constraints,
- communicating capacities and constraints to stakeholders,
- collaborating on mitigation plans among public and private stakeholders,
- resource alignment,
- unity of effort to relieve system constraints and increase transportation system capacities.

continued on page 71

U.S. Trade Recovery Protocols

The primary objectives of U.S. trade recovery protocols are to:

- provide a forum for intergovernmental dialogues and government/private sector interaction to respond to important issues to expedite trade recovery and restore the continuity of commerce;
- assist senior-level decision makers by ensuring they understand the status of the national transportation system, so they can provide informed direction to the actors in a trade recovery scenario;
- provide those same decision makers with recommendations for national-level priorities for transportation system recovery and trade resumption/continuity.

The Process

There are six steps to the trade recovery protocol process:

- **initiating protocols,**
- **collaboration on the initial assessment of the incident,**
- **developing mitigation strategies and plans,**
- **implementing mitigation strategies and plans,**
- **managing mitigation strategies and plans,**
- **protocol deactivation.**

Initiating protocols. Before activating the protocols, the appropriate authorities from the U.S. and its affected trading partners consult and agree to the initiation. At such time as it is agreed to activate them, the operations centers of both countries have the responsibility to:

- provide the communications capabilities required for protocol implementation;
- collect and share relevant information related to the incident that is applicable to joint trade recovery matters.

Initial assessment collaboration. The partners activate their respective internal maritime trade recovery processes and convene a conference call to share their respective governments' assessment of the situation.

Developing mitigation strategies and plans. At this step, the parties use their existing internal maritime trade recovery processes even after a determination has been made that an event in one country or both countries could or does significantly disrupt the flow of trade and/or passengers between them. The countries also provide representatives to participate in each other's trade recovery processes.

Implementing mitigation strategies and plans. Each country will consult on its ability to support the maritime aspects of internal mitigation plans. In those instances where mitigation plans can be fully supported, each country will indicate whether doing so requires redeploying resources. If it does, the party or parties needing to realign resources will attempt to harmonize the time frame and alter the overall mitigation plan as necessary.

Managing mitigation strategies and plans. The partners continuously convey new information to their communication centers, and provide information from other sources to monitor and adjust the status of the overall capability to handle passengers and cargo. Continuous monitoring, updating, and sharing of situational awareness information ensures that national-level senior government leaders have the most current information to best facilitate and collectively manage recovery.

Protocol deactivation. Deactivation will be coordinated among participants as the need for trade recovery incident management recedes.



Coast Guard vessels sit tied to the remaining docks following Hurricane Ike, at Coast Guard Sector Field Office Galveston, Texas. The SFO units remained operational, and aids to navigation units replaced the aids to navigation destroyed by the storm. U.S. Coast Guard photo by Petty Officer Rob Simpson.

Most response management systems in the U.S. rest upon the foundation of state and local governments being first on scene. Under the precepts of the U.S. National Response Framework, federal government support is provided when state and local resources are overwhelmed, or when an incident spans multiple jurisdictions.

The Basic Phases of a Recovery Process

Although there will be some differences based on the type of event and location, governments and the private sector will go through several phases to achieve recovery:

- response,
- stabilization,
- intermediate recovery activities,
- long-term recovery,
- trade recovery.

Response activities are the actions that mitigate the damaging effects of an event—like ensuring basic human needs are met and maintaining the infrastructure necessary to move goods and people. As response activities conclude, stabilization efforts then manage and contain the event’s immediate impact on community systems, including activities like providing essential health and safety services, ensuring that transportation routes remain clear, and removing debris.

Intermediate recovery activities involve taking actions that return people, critical infrastructure, and essential government or commercial services back to a functional state. Such activities are characterized by temporary actions that provide a bridge to permanent measures like returning displaced persons to

their community or developing impact assessments of key resources.

Long-term recovery may continue for months to years. A long-term recovery plan establishes the process of rebuilding damaged or destroyed social, economic, natural, and built environments in a community to everyday conditions.

Trade Recovery Responsibilities, Priorities

U.S. protocols have a pre-planned communications system with pre-identified contacts within the government and

the carrier and trade segments of the private sector. This helps manage trade recovery priorities for goods, people, and conveyances.

Chief Petty Officer Charles Gittings mans a tagline to control the crate being transferred to the CGC *Oak* for disaster relief. U.S. Coast Guard photo by Petty Officer Brandyn Hill.



For example, goods and people can be prioritized in the following order:

- those required to support response and recovery operations,
- those identified as national priorities,
- those participants in trusted trader and trusted traveller programs,
- everything and everybody else.

For conveyances, prioritization could be based on different factors, including:

- vessels with a history of compliance with laws, policies, and procedures;
- cargo vessels participating in known shipper programs;
- vessels with no identified crew or passenger security concerns.

Communications with Foreign Trading Partners

Incidents may require consultation with foreign trading partners to address bilateral priorities or

temporarily control the flow of non-priority cargo. Once international partners establish the initial trade recovery dialogues, they should continue until the transportation system has returned to a state that allows for resumption of long-term operations.

The U.S. will continue to build upon its trade recovery processes. However, to have a truly effective global system, other governments (with the assistance of international organizations where appropriate) must develop their own protocols to produce the most effective global response to disruptions in trade.

About the author:

Ms. Louritha Green is a 2010 Ian Axford (New Zealand) Fellow. She holds a Juris Doctor from Tulane University Law School, a Master's degree from Harvard University, and a Bachelor's degree from the University of Arkansas. She has worked with Customs and Border Protection as an attorney and international trade liaison.

A U.S. Coast Guard team assesses a pier damaged in the wake of a hurricane. U.S. Coast Guard photo by Petty Officer Sabrina Elgammal.



Lessons Learned

from **USCG Casualty
Investigations**



Costa & Corvo



Cape Horn

***A regular feature in Proceedings:
“Lessons Learned From USCG
Casualty Investigations.”***

In this ongoing feature, we take a close look at recent marine casualties. We explore how these incidents occurred, including any environmental, vessel design, or human error factors that contributed to each event.

We outline the U.S. Coast Guard marine casualty investigations that followed, describe in detail the lessons learned through them, and indicate any changes in maritime regulations that occurred as a result of those investigations.

Unless otherwise noted, all information, statistics, graphics, and quotes come from the investigative report. All conclusions are based on information taken from the report.

Lessons Learned

from **USCG Casualty Investigations**

Night Shift

A broken autopilot and sudden loss of stability leave a fishing vessel's crew fatally shorthanded.

by Ms. CAROLYN STEELE
Technical Writer

The skies were clear and the seas calm off the coast of Massachusetts that night in early November of 2008. The crew of a fishing trawler observed the glow of a nearby sister vessel's lights as it hauled in the day's catch. Without warning, those lights abruptly vanished, replaced by an eerie darkness.

What Happened

At 9 a.m. on November 9, 2008, the 71-foot fishing vessel *Costa & Corvo* departed New Bedford, Mass., for a routine ground fishing trip about 118 miles east of Nantucket with three crewmembers and a captain aboard. At some point over the next three days, the vessel's autopilot stopped functioning and crewmembers unsuccessfully tried to fix the problem. However, the captain decided to continue with the trip—possibly because the forecast called for calm weather.



Costa & Corvo.

By 7 p.m. on November 12, 2008, the net was filled, so the crew had begun dragging their fishing gear to haul in the catch. At around 11 p.m., a sister vessel, the *Mary K*, passed within 400 yards and saw that the dragger's lights were fully illuminated.

By midnight, the crewmembers had completed a successful haul and were lowering a fully loaded net onto the vessel's stern. Moments later, events took a catastrophic turn.

The heavy net, slippery with live catch, suddenly shifted to the port side deck and caused the vessel to roll to port. In a rapid chain reaction, the unsecured port trawl door became submerged and fell open, directing seawater onto the vessel's deck and further degrading its stability. Within minutes the boat listed, then capsized to port.

Vanished Vessel

At 12:05 a.m. on November 13, 2008, the crews of two other nearby fishing vessels contacted the *Mary K*, stating they had heard crashing sounds over the VHF radio, and the captain promptly relayed this information to Coast Guard Sector Boston, adding that he could no longer see his sister ship, whose lights had disappeared just moments before.

These conversations were interrupted by a distress signal from the emergency position-indicating radio beacon (EPIRB) registered to the downed vessel. The *Mary K*'s captain noted that the distressed vessel remained on radar, so the Coast Guard directed him to proceed to the vessel's last known position. The

other two nearby boats also headed toward it. Meanwhile, Coast Guard and other vessels in the area continued unsuccessful attempts to contact it by radio.

Help Arrives

At 12:45 a.m. the *Mary K* arrived on the scene and its crew saw that their sister vessel had capsized. Hearing cries from the water, they saw three men clinging to two life rings, and they pulled the men from the frigid water. All three were dressed in light clothing; none wore a life vest or survival suit. The survivors told their rescuers that they had last seen the captain entering the pilothouse just as the vessel began to list to the port side and roll. The *Mary K's* captain relayed this information to the Coast Guard, then searched for the missing captain.

Five minutes later, Coast Guard Air Station Cape Cod aircraft arrived on the scene and joined in the search for the missing captain. By 1 a.m., a Coast Guard Air Station Cape Cod helicopter arrived and lowered emergency medical technicians onto the other fishing vessel to evaluate the three survivors. All seemed to be in good health.

At 1:30 a.m. on November 13—one and a half hours after initially losing stability—the capsized fishing vessel sank. Coast Guard crews searched for the captain for more than 30 hours and covered more than 280 square miles, but never found him. These efforts were halted at 9:41 p.m. on November 14, 2008. The captain was presumed dead.

Coast Guard Analysis

Coast Guard investigators used crew testimony as well as underwater images of what is believed to be the fishing vessel resting on the ocean floor to help determine the probable cause of the accident—a sudden and dramatic decrease in the vessel's stability.

Prior to retrieving the net, the crew of the vessel had closed all freeing ports and scupper devices¹ to prevent loss of the catch. The pilothouse and engine room doors had been left open. In addition, the pilothouse and helm were left unmanned while all members of the crew, including the captain, worked on deck hauling in the catch. The vessel—with no autopilot—was moving forward at a speed of two to three knots.

As the fully loaded net was lowered, it abruptly shifted, causing the entire vessel to list severely to port. The sudden shift intensified as the port trawl door, which was only loosely secured to the port rail just above the waterline, submerged and directed sea-

water onto the deck. With scuppers and freeing ports closed, the water remained on the deck and drove the vessel further to port. These events combined to make the vessel lose stability and capsize.

Before the crew had retrieved the fully loaded fishing net, the weight of the catch dragging underwater had kept the vessel on a steady heading. However, once the net was taken out of the water, the vessel's heading was suddenly subject to changes caused by waves and wind. The autopilot was broken and the captain had left the vessel's helm unmanned, so there was no way to make rudder adjustments to counter these movements. Once the vessel began to roll to port, it continued over until it capsized.

Non-Contributing Factors

A variety of issues were considered in the Coast Guard investigation to determine the cause of this accident. Ironically, the veteran crew had followed numerous safety protocols before the voyage.

Weather—At the time of the accident, the weather conditions were clear, with light winds, 12 nautical mile visibility, and seas between one and three feet. The air temperature was 47° Fahrenheit, and the water temperature was 53° Fahrenheit.

Crew Experience—The captain and crew were seasoned mariners, with a total of 100 years' experience in the fishing industry among them. In addition, both captain and crew had served aboard the vessel numerous times, so they were familiar with the boat's limitations, handling abilities, and characteristics.

Safety Precautions—The captain and two of the crewmembers had recently attended a safety and survival workshop, and during a Coast Guard voluntary dockside examination three days before the incident, the vessel's training records showed that all crewmembers had conducted monthly emergency drills and familiarization training. Their monthly records of EPIRB inspections and tests were current.

Material Condition of the Vessel—Interviews with surviving crewmembers and review of a recent condition and value survey revealed no previous unsafe material condition aboard the fishing vessel before the fateful breakdown of the autopilot.

Deployment of Lifesaving Equipment—Both the life raft and EPIRB were functioning properly at the time of the accident. A crewmember deployed one life ring; the other two life rings floated free of the



vessel. That notwithstanding, crewmembers were not wearing survival suits or life jackets at the time of the accident, so they had no time to don them when the vessel capsized so suddenly.

Contributing Factors

Human Error

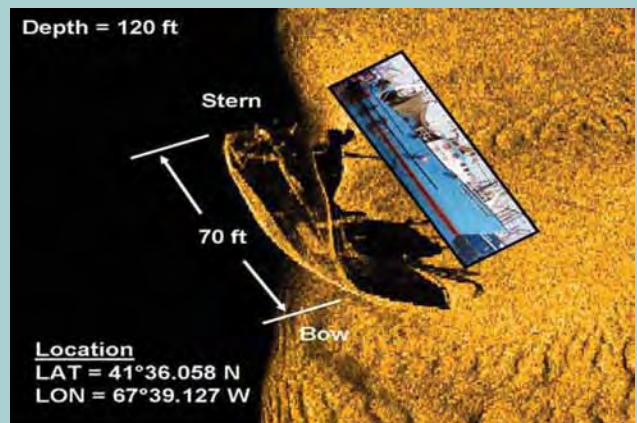
Task Preparation Deficiencies—It is customary on a fishing vessel to close the freeing ports and scuppers when a net is hauled in to prevent loss of catch.

However, it is improper to leave the engine room and pilothouse doors open, and this error contributed to the flooding of the vessel. To make matters worse, the trawl door was only loosely secured to the port rail when the catch was hauled onto the deck, falling open as the vessel listed to one side, allowing water to flood the port side deck.

Situational Awareness—The crewmembers, focused on hauling in their catch, were not fully aware of the seri-

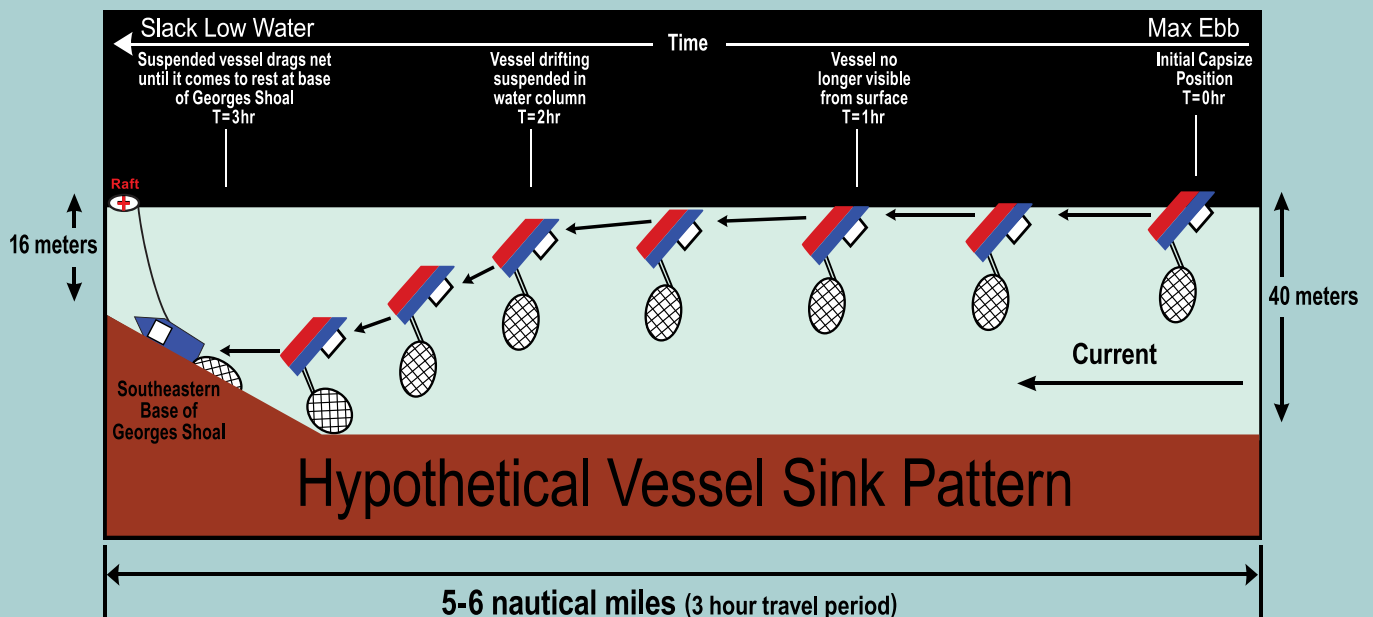
Underwater Survey

A survey conducted near the last known position of the downed vessel found what is most probably the *Costa & Corvo*. A hypothetical vessel sink pattern was derived from the position of the vessel when the crew was recovered and the location that the life raft was located after the vessel sank.



Sunken vessel located near last position of the fishing vessel.

It is believed the vessel slowly slid down the slope of George’s Shoal and came to rest in 120 feet of water. From the sonar images, it is clear that the vessel is lying on its port side. As imaged from the starboard side, the vessel hull appears to be intact and complete.



Hypothetical vessel sink pattern. Images courtesy of the Naval Undersea Warfare Center of the Naval Sea Systems.

ous impact that the shifting of the fully loaded fishing net on deck would have on the vessel's stability. They were caught completely off-guard by the sudden loss of equilibrium that led to the vessel's capsizing.

Errors in Judgment—The vessel's captain made two critical blunders. The first was in deciding to proceed with the voyage in spite of a broken autopilot. The second was in leaving the pilothouse to help the crew on the main deck retrieve the loaded fishing net. Leaving the helm unmanned and the engine engaged meant that the vessel's course was subject to alterations caused by hauling in the fishing gear, heeling moments, tidal currents, waves, and wind. Thus began the deadly chain of events that led to the vessel's capsizing.

Lessons Learned

Fishing is one of the most hazardous professions in the world, outranking other high-casualty industries such as timber cutting and logging, firefighting, law enforcement, and professional motor vehicle operators. More than 100,000 fishing vessels operate in the U.S. fleet; 1,903 vessels and 934 lives were lost from 1992 to 2007.² To bring down these numbers, fishermen need to exercise safety precautions even more diligently than other mariners.

Set the proper priorities.

The vessel had no inherent safety problems other than the broken autopilot. It is possible that the captain, not wanting to waste time and resources by turning back, continued with the voyage despite the malfunction. He also left the pilothouse to help his crew haul in the catch—a fatal error in judgment.

Haste makes waste.

Most likely in a hurry and distracted by other tasks, crewmembers left the doors to the pilothouse and engine rooms open, allowing more water to flood into the vessel and making a bad situation worse. In addition, they did not properly secure the trawl door to the port rail, causing even more water to flood onto the vessel as it became unstable.

Don't take anything for granted.

The stability of a fishing vessel is not a constant; it undergoes continuous changes in the course of each voyage. A stable vessel may become unstable because it is improperly loaded and operated, or if its equipment malfunctions.

Acknowledgment:

Proceedings gratefully acknowledges the support of CAPT David Fish, Mr. Tim Farley, and Mr. Ken Olsen of the U.S. Coast Guard Office of Investigations and Casualty Analysis.

About the author:

Ms. Carolyn Steele has more than 20 years of experience in the communications field. As a writer/editor she has worked on numerous Coast Guard projects since 2006, including the USCG Marine Safety Manual, the USCG Maritime Law Enforcement Manual, and USCG Publication 1. She is also the editor and designer of the Crew Endurance Management newsletter, and designs the Coast Guard's VRP Review newsletter. Ms. Steele has an extensive background in fine art and graphic design.

Endnotes:

- ¹ Freeing ports are large openings in the rail (bulwarks) just above the deck that allow the ship to clear itself of water when seas break over the deck. Scuppers are openings in the side of a ship at deck level that allow water to run off. Closing the scuppers is standard practice to prevent the loss of catch over the side when a fishing net is to be opened on deck and the catch sorted.
- ² "A Review of Lost Fishing Vessels & Crew Fatalities, 1992–2007;" USCG Office of Investigations and Analysis.



Lessons Learned

from **USCG Casualty Investigations**

Lethal Lifesaver

Carbon dioxide saves a ship but claims two lives.

by Ms. CAROLYN STEELE
Technical Writer

In the early morning hours of March 31, 2002, a fire broke out in the engine room of the M/V *Cape Horn*, which was approximately 645 nautical miles north-east of Honolulu, Hawaii. Though the fire caused extensive material damage, it was contained before it spread to other parts of the vessel. The fire destroyed expensive equipment, but ensuing events caused damage that cannot be assigned a price tag—the loss of human life.

Background

The vessel is a roll-on/roll-off (RoRo) ship, designed to carry vehicles and equipment to support humanitarian and combat missions. These ships have a cargo carrying capacity of more than 380,000 square feet—equivalent to almost eight football fields.

Two weeks before the accident, the vessel had been activated from reduced operational status in San Francisco to participate in a military exercise. On March 31, 2002, it was en route from San Francisco to Pearl Harbor, Hawaii, carrying a cargo of military vehicles and ammunition.



M/V *Cape Horn*.

Sequence of Events

The Fire—During the midwatch, the third assistant engineer noticed a small leak in the No. 9 cylinder fuel oil return line. He would later state he notified the chief engineer of the leak, and this information was passed to the second engineer during the watch relief. However, no attempt was made to fix the problem at that time.

At 5:53 a.m., the ship's engineering automated read-out log showed a sudden series of alarms. The second assistant engineer on watch saw smoke filling the engine room. He called the bridge and left the area with another crewmember without pushing the emergency engine cut-off switch. The chief mate sounded the general alarm and awakened all crewmembers, including the captain, who assumed control of the bridge.

At 5:56 a.m., the engineering automated log showed that the main engine remote control shutdown had been activated.

Failed Attempts to Close the Machine Shop Door—At 5:58 a.m., the second engineer started the emergency diesel generator, as instructed by the chief engineer. In preparation for releasing carbon dioxide (CO₂) to combat the fire, the chief mate, chief engineer, and assistant engineer went to the machine shop to close the sliding watertight door and contain the fire. However, they were unable to do so because the door had been jury-rigged with a T-handle to jam it open. With thick billowing smoke filling the space, they retreated.

Meanwhile, the other crewmembers proceeded to their assigned fire stations. The chief mate took a muster, ordered boundary cooling of the lower deck bulkheads, and ordered the engine room vents closed. The chief mate ordered the second mate to



Machine shop door, dogged open.

stage firefighting gear on the main deck (deck 4) outside the guillotine door leading to the main ramp.

The second assistant engineer went to deck 5 to close the ventilation dampers on the port side of the stack bulkhead. He discovered that three of the five damper handles were in the “open” position. When he tried to close them, two of the handles snapped off. Later examination showed that even though badly rusted, the handles had been painted over.

At 6 a.m., the bridge watch sent a Mayday call. Twenty minutes later, the chief mate and boatswain’s mate descended the main ramp to survey the fire. Brown smoke was billowing out of the machine shop, again preventing them from closing the door.

Crewmembers wearing self-contained breathing apparatus (SCBAs) made a third attempt to close the machine shop door. Smoke and poor visibility again hampered their progress. After about 10 minutes, one crewmember’s low air alarm went off, forcing the team to retreat before they could reach the jammed-open door.

Carbon Dioxide Release—The captain, the chief mate, and the chief engineer discussed releasing carbon dioxide from the ship’s fixed firefighting system. Because the machine shop door was still open, they believed that CO₂ would be released into both the engine room and deck 3, reaching the entire blaze if the fire had spread beyond the engine room. Before releasing the CO₂, the chief mate took a mus-

ter to account for all crewmembers.

At around 6:45 a.m., nearly an hour after the fire alarm sounded, the captain tried to enter the CO₂ room, but he, too, encountered a veil of smoke. He donned an SCBA and re-entered the room. The captain then unintentionally released CO₂ into *hold 3*, thinking he was releasing the CO₂ into the *deck 3* engine room.

The captain returned to the bridge and was relieved to see white smoke coming from the stack and purifier room vent on deck 6; the smoke had previously been black. Despite the misdirected discharge of CO₂ into hold 3, the white smoke indicated that the fire had been successfully extinguished.

The captain returned to the bridge and was relieved to see white smoke coming from the stack and purifier room vent on deck 6; the smoke had previously been black. Despite the misdirected discharge of CO₂ into hold 3, the white smoke indicated that the fire had been successfully extinguished.

After the Fire

The following account is based on the recollections of various crewmembers after the fact. Because visibility was at times poor, and several of the men were likely suffering from the effects of smoke and CO₂ inhalation, there was some confusion about the exact times and sequence of events.

The captain, chief mate, and chief engineer discussed the need to re-enter the engine room to establish the status of the fire and assess the ship’s ability to get underway. They also discussed how long to wait to enter the engine room after the CO₂ release. The chief engineer was concerned about the fact that the vessel was hundreds of miles from land with a cargo of ammunition. He was anxious for the crew to “bring the ship back to life.”

For the next hour, crewmembers performed boundary cooling and pre-staging of firefighting equipment to prepare for re-entry into the engine room. During this time the captain, chief mate, and chief engineer planned



Valve release diagram and valve releases for engine room and hold 3.



the route and equipment needed, and divided crewmembers into three teams:

- primary—the chief mate and chief engineer;
- secondary—the first assistant engineer and a third assistant engineer;
- backup—an able-bodied seaman and another third assistant engineer.

The captain, aware of the dangers of CO₂, issued a specific order that teams were not to enter the lower level of the engine room. Carbon dioxide is heavier than air and would be more concentrated at lower levels of the vessel.

The second mate was tasked to keep a log of entry/exit times and other specific events, but was unable to do so because he did not have a wristwatch. One of the military personnel aboard assisted him as a timekeeper to track how long entry teams were “on air.”

After donning their SCBA gear, teams entered from the deck 4 starboard stairwell and descended to the machine shop. In the events that followed, several crewmembers experienced frequent radio communication loss. In fact, during the communications check when the chief mate initially tried to speak through his SCBA mask, the transmission was so garbled that he continually lifted his mask when speaking into the radio.

The backup team manned the hose, the secondary team advanced toward the machine shop watertight door, and the primary team continued on through the machine shop onto the platform overlooking the engine room. From here they saw that the fire appeared to be extinguished, which they reported to the captain at 6:04 a.m.

At 6:15 a.m., the primary and secondary teams changed out their SCBA air tanks and entered the starboard stairwell, intending to check on the status of the fire. The backup team remained on deck 4 without donning SCBAs. The primary and secondary teams passed the electrical workshop and descended

the stairwell into the engine room. They were not using safety lines to tether team members together.

Man Down

From this point on, the account of events becomes somewhat murky because no timeline was logged for most activities. Therefore, much of the following cannot be verified.

The secondary team remained at the base of the stairwell next to the engine control room while the primary team went around the aft end of the main diesel engine. The chief engineer felt residual heat and could see damage from the fire in the aft port side of the main diesel engine. He had gone to the top of the port side stairwell leading down into the lower deck of the engine room and was looking down when he lost consciousness and fell, landing on a small platform at the bottom. It is not clear what caused the fall.

At 6:30 a.m., seeing his unconscious teammate at the foot of the stairs, the chief mate stated “man down” over the radio and descended the staircase alone to help the fallen man. Upon hearing this transmission, the captain ordered the backup team into action.

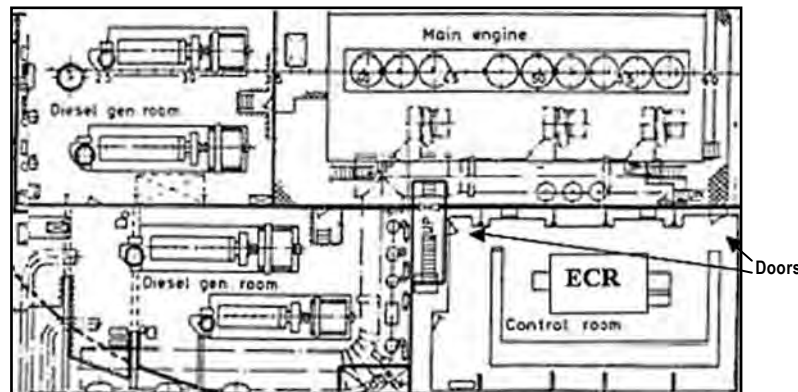
They donned SCBAs and proceeded to the lower decks. A short time later, the third assistant engineer, who was on the secondary team, went back up the stairs to get more help.

The chief engineer regained consciousness. He was lying alone where he

had fallen (on the platform next to the entrance to the emergency escape trunk) and was wearing an emergency life-saving apparatus 10-minute air pack, which the chief mate presumably placed on him. The chief engineer was able to open a nearby escape trunk door and climb to safety. He rejoined the crew at the starboard side and was administered oxygen by the ship’s medical officer. His escape was not communicated to the other teams.

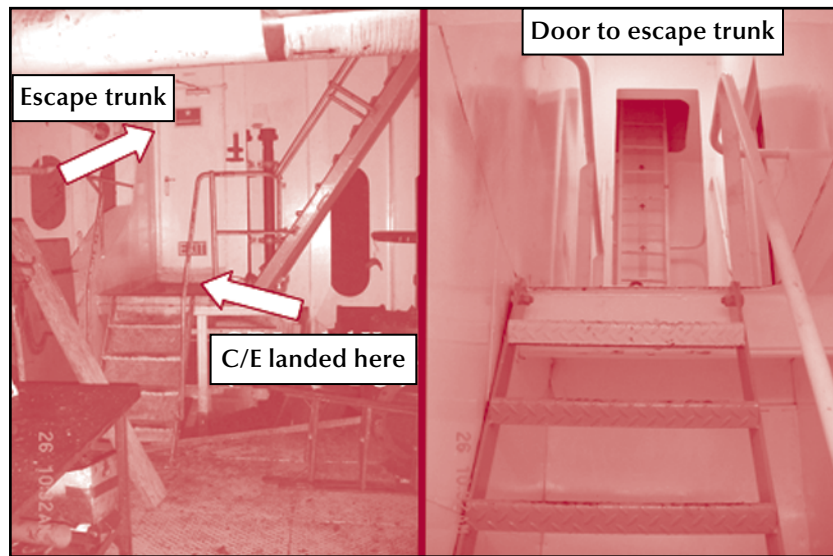
Men Down

In the meantime, not realizing the chief engineer had recovered and was safe, the other designated team members continued their attempts to recover him.



Engine room diagram. Location: second platform deck.

An electrician (not assigned to any team) also donned an SBCA mask and descended the stairs alone to deck 2. He found the chief mate unconscious on the deck behind the stair tower at the aft end of the main diesel engine. He saw the chief mate's air gauge read "empty." The chief mate was unresponsive, and his pupils were fixed and dilated. The electrician then found the first assistant engineer also lying unconscious on the ramp leading down to the port side of the engine room. He too was unresponsive; his air gauge also read "empty."



Where chief engineer fell down stairwell and proximity of escape trunk. Photo on right shows view through door to escape trunk.

While the electrician was trying to help the first assistant engineer, the backup team found the chief mate lying behind the stair tower with no pulse. The backup team quickly changed out the chief mate's air tank with an extra tank they had brought and attempted to move him to safety. They were unable to do so because both of the backup team members' low-air alarms began to sound, so they were compelled to leave the area.

At 10:05 a.m., after several team efforts, the unconscious first assistant engineer was brought into the port side escape trunk. Two crewmembers administered CPR. He was then placed in a litter and hauled up through the trunk to deck 4. For the next hour and a half CPR was performed on him—unfortunately, to no avail.

Because of limited air time and exhaustion, it took several rescue team attempts to carry the chief mate up the stairwell to deck 4. CPR efforts continued on him for an hour, but at 12:05 p.m. they were halted because he could not be revived.

Post-Casualties

At 2 p.m., the M/V *Mohihana* arrived to respond to the Automated Mutual Assistance Vessel Rescue system alert. It left the scene at 3:45 p.m. because the captain of the damaged vessel said that help was not needed.

At 2:30 p.m., the bodies of the two crewmembers were placed in a cold storage facility aboard the RoRo vessel.

At 4 p.m., the captain ordered a team to be assembled to enter the engine room, assess the status of the engine room, and ensure the fire was out. A primary

and backup team donned SCBAs, explored the entire engine room, and found no continued threat of fire. The captain then ordered the engine room ventilated.

The vessel established communications with USNS *Shasta* and Hawaiian Tug and Barge. The USNS *Shasta* ship arrived on Monday, April 2, and began towing the damaged vessel. The tug *Hoku Kea* arrived on Wednesday morning and took over towing duties.

The RoRo vessel arrived at her destination—Pearl Harbor, Hawaii—on Friday, April 4, 2002. The ship had sustained \$1,984,250 of damage to its engine room.

Autopsies performed on the two crewmembers stated that the cause of death was asphyxia due to oxygen deficiency combined with CO₂ inhalation. Both deaths were deemed accidental.

What Went Wrong

The fire and resulting deaths of two men were caused by a combination of human error and mechanical failures. Obviously, a fire aboard a ship carrying ammunition is a serious enough casualty in itself, but what happened after the fire was put out turned a costly accident into a tragedy.

Based on its examination of the ship after the accident and its review of crewmembers' statements, the Coast Guard was able to piece together and analyze the events that led to this tragedy. One fact emerged for investigators: The fire and resulting deaths of the crew rescue were due to a combination of factors, not the result of a single human error or mechanical failure alone.

Equipment Failure

- **Leaking pipe**

The first link in the disastrous chain of events was inadequate maintenance on the ship. The fire started when mist from a leak in a pressurized fuel oil return line came into contact with a heat source (a turbocharger or electrical panel) in the engine room. The leak itself was the result of a poorly brazed joint where improper filler material was used for the repair when the vessel had last been in dry dock. When the joint failed, pressurized fuel oil escaped from the fitting.

- **Broken damper handles**

Coast Guard inspectors later found that three of the five damper control handles were broken, the third failure having occurred when one of the dampers was reopened after the fire. They were rusted through and painted over, had not been greased, and were full of sandblast grit, causing some parts to become stuck in position. Further, the open/closed positions of one damper control had been marked backward.



Broken damper controls and improperly marked control.

- **Substandard radio devices**

Crewmembers' SCBA masks did not have integrated communications. This led the chief mate to raise his mask while speaking. Several crewmembers would later note that communications were made difficult by the design of the equipment, and that they often had to repeat themselves because of ineffective transmission.

- **Defective SCBAs**

All but one of the teams' SCBAs later failed at least one of the National Institute for Occupational Safety and Health tests for conformance to federal performance requirements.

Human Error

- **Faulty communications**

The third assistant engineer on the 4 to 8 a.m. watch first noticed the oil leak. He would later state that he notified the chief engineer, who at the time was repairing the No. 2 cylinder fuel oil return line. However, the chief engineer told the Coast Guard that he never heard about the No. 9 cylinder leak. For whatever reason, critical information about the leak was never passed on to the next watch, so nothing was done to address it at the time.

- **Critical oversight**

Though the second engineer was the first person to see smoke filling the engine room and called the bridge to sound the general alarm, he failed to shut down the vessel's main engine. Though it was shut off from the bridge a few minutes later, in an emergency involving fire—especially one on a vessel carrying ammunition—every second counts.

- **Safety breach**

The sliding machine shop door was jury-rigged with a T-handle to keep it jammed open. Crewmembers stated that the door was kept open most of the time while the ship was underway to allow ease of access.

- **Lack of familiarity with the vessel's controls**

The captain unintentionally released CO₂ into hold 3 near the bow of the ship, rather than deck 3, which

was immediately forward of the engine room and was the intended target of the CO₂ release.

- **Errors in judgment**

Though the station bill designated the chief mate as "at scene in charge," he personally participated in the primary emergency team with the chief engineer. His personal involvement contributed to a breakdown of command and control when he devoted his full attention to the aid of a fallen member of the crew, the chief engineer.

The second mate, who was tasked with timekeeping and logging of entry teams, did not wear a

wristwatch, which threatened direct and immediate communications and compromised the safety of all involved.

After the casualties, the captain declined assistance from the first vessel to arrive on the scene despite the recent loss of two crewmembers and the fact that no final fire assessment had been performed on the engine room.

- **Flawed contingency planning**

The backup team on the first post-CO₂ fire assessment/entry was on air at the same time as the primary and secondary teams. This reduced the effectiveness of backup efforts in the event of an emergency, where all teams would have expended the same amount of air. Essentially, there was no real “backup.”

- **Lack of organization**

On the second re-entry to the machine room after the fire was extinguished, the backup team stayed on deck 4 off-air but did not don their SCBAs, which delayed their ability to respond when called on to do so. Further, the teams did not use lifelines. Had they done this, they might have averted the tragic series of events that began when the chief engineer fell down the stairs.

- **Failure to follow orders**

The chief mate as well as members of the other teams disobeyed the captain’s orders by descending into the lower level of the engine room to look for their crewmate, who had fallen down the stairs.

Questions and Possible Answers

- *Why wasn’t there an immediate response to the leak in the No. 9 cylinder fuel oil return line?*

The chief engineer would later testify that he had not been told about the leak. Perhaps the third assistant intended to tell him, or thought he had told him, but in fact did not. Perhaps the chief engineer may not have registered the information because he had been repairing a leak on the No. 2 cylinder fuel oil return line at the time he was told about the leak. Whatever the reason, the information was not passed on.

- *Why was the machine room door dogged open?*

The ergonomic design of the door was very poor. One crewmember told USCG investigators that the sub-hatch of the door was a “shin buster.” Crewmembers were unable to easily pass this area without bumping into a sharp edge, so they kept it open for easy access.

- *Why were the ventilation damper handles in such poor condition?*

It is possible this ship’s state of preparedness was compromised because she had only recently been activated from reduced operational status to ready reserve status.

- *Why did the chief engineer fall down the stairs, triggering the second, tragic series of events?*

When questioned by Coast Guard investigators, the chief engineer seemed unclear about what had caused him to fall. He offered different explanations, such as “On the first or second step, I either slipped or (the) mask seal failed” and “I went to sleep or fell asleep.” It is possible that he inhaled enough CO₂ to make him lightheaded or disoriented, causing him to lose his balance or pass out. Additionally, since teams were not using safety lines, his fall was unimpeded, making it easy for him to become separated from the others.

- *Why did the captain release CO₂ into the wrong area of the vessel?*

This mistake may have been partly because the CO₂ controls included labels for ship’s holds and decks rather than just simply the ship’s decks, the more common reference point for mariners.

- *Why did team members enter the lower level of the engine room, in violation of the captain’s orders?*

The men were likely responding to a human instinct to help a fallen crewmember without pausing to think about the captain’s instruction or danger to themselves.

- *Why didn’t the two men who died realize that the escape trunk was also nearby?*

Both victims were found only a couple of feet from the escape trunk, which would have led them to safety. They were no doubt overcome by CO₂, which even at a lower concentration can cause confusion and disorientation.

- *Why did the crew fail to use the buddy system?*

The chief mate descended to the lower engine room alone to check his fallen teammate. The third assistant engineer returned to the staging deck alone. One possible explanation for this is that this ship’s crew did not take time during the two weeks after they were put on ready reserve status to perform multiple emergency and fire drills before they began their voyage from San Francisco.



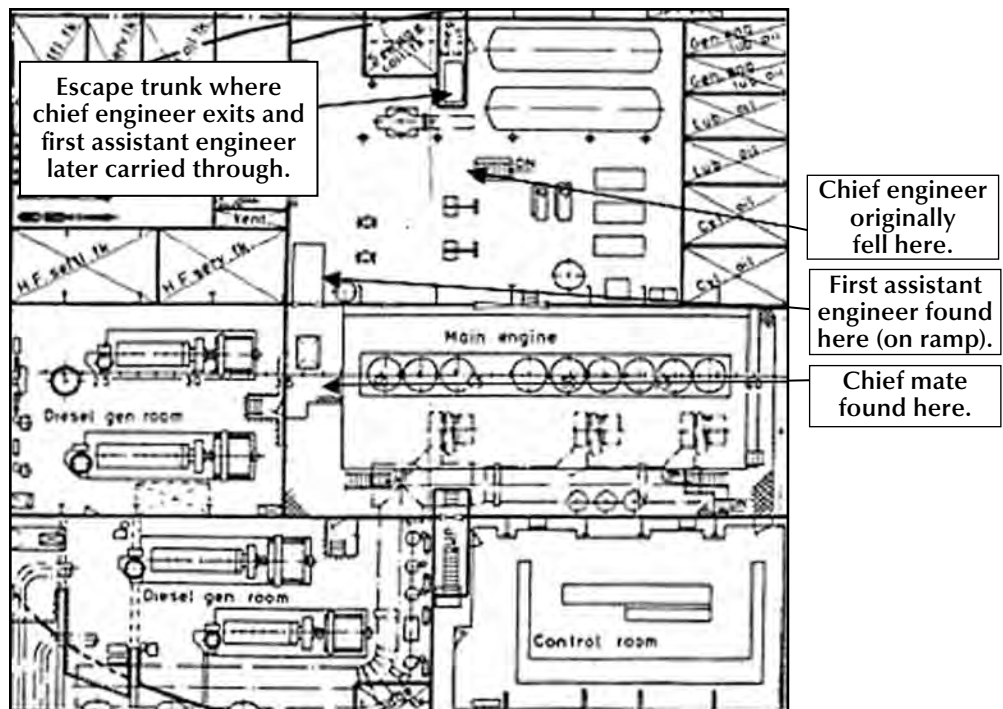


Diagram of engine room, noting locations where chief mate and first assistant engineer were found.

Assessment and Lessons Learned

Though it did not indict any single factor or individual as being to blame for the tragedy, the USCG report went on to state:

“An inadequate maintenance regime might better be attributed, at least partially, to those who maintained the vessel in a reserve operating status rather than the crew that actually manned the vessel at the time of the incident.”

Lessons Learned

- **Practice makes perfect.** Performing drills time and again may be tedious, but it is the only way to reduce the risk of a catastrophe. This particularly applied in the case at hand, where the ship’s cargo was ammunition.
- **Take time to think things through,** even though your first instinct might be adrenaline-based. In this case, had the first mate and second engineer stopped a moment to consider the captain’s orders not to go into the lower level of the engine room because of higher CO₂ concentrations, they might not have lost their lives.
- **Know your ship and know your shipmates.** In this case, the crew consisted of merchant mariners who had perhaps never before worked together as a team. Though ship procedures and the chain

of command are things all mariners are trained to follow, people’s work styles and methods of communication may vary tremendously from crew to crew.

- **In sufficient concentration, carbon dioxide is a lethal gas.** It can put out a fire, but it can also kill in a matter of seconds without warning. Take all possible precautions when using it.
- **When in doubt, err on the side of caution.**

Analysis

The Coast Guard’s analysis of this case points out that there was no single human error, no single mechanical failure, and no single incident where sound judgment failed.

- The crewmembers who jammed the door open did not foresee the effect this might have in the case of fire. They were saving their skins.
- The person who improperly brazed the pipe did not consider that a fuel leak could start a chain of events resulting in damage to the ship and the death of others.
- The men who risked their lives to try to save their comrade did not consider the possible results of not being tethered together, and did not respond to the limitations of their breathing apparatus. They were only focused on helping their fallen crewmember.

- The person who painted over the rusty damper handles did not stop to think that he or she might be setting the stage for equipment failure at a critical moment.

Ultimately, the lesson to be learned from this tragic incident is not something that can be turned into a simple axiom or phrase like “Always check your gear.” Rather, it illustrates how every safety procedure affects another. A series of failures will escalate the danger and diminish the ability to halt the problem. The Coast Guard’s report expressed it as follows:

“Expert analysis of system accidents reveals a common trait: Tragedies do not result from a single factor, either human error or mechanical failure. Complex systems, such as the maritime transportation system, simply possess too many proven defenses for a single factor to pose a significant threat in itself. Instead,

major tragedies appear to result from a strange and unforeseen combination of events and factors, each occurring at exactly the right time and place to enable the next. Together, the threats build or synergize; each single factor is necessary because the accident couldn’t happen without it, but insufficient without the others.”

Acknowledgment:

Proceedings gratefully acknowledges the support of CAPT David Fish, Mr. Tim Farley, and Mr. Ken Olsen of the U.S. Coast Guard Office of Investigations and Casualty Analysis.

About the author:

Ms. Carolyn Steele has more than 20 years of experience in the communications field. As a freelance writer/editor she has worked on numerous Coast Guard projects, including the USCG Marine Safety Manual, the USCG Maritime Law Enforcement Manual, and USCG Publication 1. She is also the editor and designer of the Crew Endurance Management newsletter.



Understanding Methyl Ethyl Ketone

by LT SEAN PETERSON

U.S. Coast Guard Hazardous Materials Standards Division

What is it?

Methyl ethyl ketone (also known as MEK), is an organic compound found in many household products. It is commonly used in the manufacture of plastics, textiles, coatings, rubber-based industrial cements, printing inks, bonding agents, and magnetic tapes. The compound is an effective and common solvent that contributes to its main application as a low-boiling solvent for nitrocellulose, acrylic, and vinyl surface coatings. The paints and coatings industry accounts for over half of the global demand for MEK.

How is it shipped?

MEK is a colorless liquid at room temperature and normal atmospheric pressure, with an odor similar to acetone. Liquid methyl ethyl ketone is typically transported by truck, train, plane, barge, or ship.

Why should I care?

Shipping concerns.

MEK is categorized as a Category Z noxious liquid substance.¹ This means that it is deemed to present a minor hazard to either marine resources or human health.

This product has a very low flash point of -9 degrees Fahrenheit and can ignite at room temperature. It should also be noted that water is not recommended to be used to fight a fire involving this product, since it can cause the hot chemical to splatter and/or cause the fire to spread. Instead, it is recommended to use CO₂, alcohol foam, or dry chemical to fight MEK fires.

Additionally, MEK is reactive with oxidizing agents, acids, and alkalis, in some cases posing a risk of explosion. Therefore, methyl ethyl ketone should not be stored near these products.

Health concerns.

Methyl ethyl ketone has the potential to be harmful and may cause irritation to the skin, eyes, and respiratory tract, leading to itching, and pain. Ingestion may cause disruptions to the gastrointestinal tract with symptoms such as nausea, vomiting, or diarrhea. Inhaling MEK at high concentrations may cause

central nervous effects, including headache, dizziness, unconsciousness, and even coma.

While handling MEK workers must use gloves, wear body-covering clothing, goggles, and a vapor respirator. It is also recommended to work in well ventilated areas while handling the compound.

Fire or explosion concerns.

MEK is flammable and has the capability to explode when in contact with the chemicals discussed previously. If the cargo is involved with a fire, the vapors and fumes are hazardous and should be avoided. It is essential for emergency responders to wear self-contained breathing apparatus and rubber over clothing (including gloves), and to combat the fire from a safe distance or protected location. The recommended method to extinguish the fire is with alcohol-resistant foam or multi-purpose foam.

What is the Coast Guard doing about it?

MEK is categorized as a "Subchapter D" cargo, regulated in 46 Code of Federal Regulations Part 30.25. This cargo is carried in tank barges and ships that are required to be inspected by the Coast Guard.

Required design and construction standards for these vessels include:

- being double-skinned,
- having spacing between the hull and the inner tank wall,
- employing individual tank manifolds and pumps to avoid cross-contamination,
- utilizing a separate tank venting facility,
- being capable of internally circulating the tanks,
- being capable of being ventilated.

About the author:

LT Sean Peterson is a chemical engineer in the Hazardous Materials Standards Division, at U.S. Coast Guard headquarters. He focuses on domestic and international regulations for the marine transportation of bulk liquids and gases. He also has a background in vessel inspections and marine casualty investigations.

Endnote:

1. "International Code for the Construction and Equipment of Ships Carrying Dangerous Chemicals in Bulk," 2007 Edition.

Nautical Engineering Queries

Prepared by NMC Engineering
Examination Team



1. The closing of the exhaust valves used on a modern, large, low-speed main propulsion diesel engine may be directly provided by _____.
 - A. mechanical pushrods
 - B. compressed air pressure
 - C. hydraulic pressure
 - D. exhaust pressure

2. When a controller with proportional position action is used to control a process, a load change will cause the controlled variable to stabilize at some value other than the set point value. The new point at which the controlled variable stabilizes is called _____.
 - A. offset
 - B. deviation
 - C. control point
 - D. load point

3. The mechanical efficiency of a particular centrifugal bilge pump is 92.5 percent. What is the smallest horsepower motor that can effectively operate this pump at a capacity of 100 gpm with a discharge head of 15 feet?
 - A. ¼ HP
 - B. ½ HP
 - C. ¾ HP
 - D. 1.0 HP

4. The main condensate pump in a steam propulsion plant discharges directly to the _____.
 - A. air ejector inter-condenser
 - B. main condenser hotwell
 - C. air ejector after-condenser
 - D. DC heater vent condenser



1. *Note: In the past, most large, low-speed, main propulsion diesel engines were valve-less, utilizing either cross-flow or loop scavenging to remove exhaust gases from the cylinder via exhaust ports in the cylinder liner. Today, large, low-speed main propulsion diesel engines primarily utilize uniflow scavenging in which each cylinder features one centrally located exhaust valve.*
- A. mechanical pushrods. **Incorrect Answer:** Medium and high speed diesels engines equipped with the conventional overhead valve arrangement utilize mechanical pushrods. The pushrod, along with the camshaft lobe, cam follower, and rocker arm are the means by which valve is opened. The valve is closed by spring force.
- B. compressed air pressure **Correct Answer:** Exhaust valves on modern, large, slow speed uniflow scavenged main propulsion diesel engines are fitted with exhaust valve actuators, utilizing fluid power for valve operation. The valves are opened under hydraulic pressure and are closed with compressed air pressure. The air actuator is sometimes called an air spring, since it performs the same function as conventional valve springs (valve closure) using compressed air.
- C. hydraulic pressure **Incorrect Answer:** As explained in choice "B" above, hydraulic pressure is the exhaust valve opening force, not the closing force.
- D. exhaust pressure **Incorrect Answer:** Exhaust gas is not a suitable media for exhaust valve operation. Exhaust gas is not high enough in pressure to close the exhaust valve.
-
2. *Note: Controllers that feature proportional action exhibit a unique behavior. The set point value, as the name implies, is the setting of the controlled process that the controller is designed to maintain. Ideally, the set point value and the actual measured value are identical. As with all process control action types, with load or demand changes the measured value will differ from the set point value. This difference is called deviation (or error), which causes a corrective response. As the controller reacts to the deviation, the controlled variable will stabilize at a value proportional to the load or demand, and it will be different from the set point value. This difference is called offset. The new point at which the controlled variable stabilizes is called the control point.*
- A. offset **Incorrect Answer:** Offset is the difference between the set point value and the control point value.
- B. deviation **Incorrect Answer:** Deviation is the difference between the set point value and the measured value.
- C. control point **Correct Answer:** The value at which the controlled variable stabilizes is called the control point. It will vary with the load or demand.
- D. load point **Incorrect Answer:** Load point is a fictitious term. The point at which the controlled variable will stabilize for a given load is called the control point, not the load point.
-
3. A. ¼ HP **Incorrect Answer:** The ¼ HP (0.250 HP) motor is too small to operate the pump.
- B. ½ HP **Correct Answer:** The ½ HP (0.500 HP) motor is the smallest horsepower motor available to effectively operate the pump. See solution below.
- Solution:** The potential energy gained by the liquid is equal to the weight of the liquid pumped, multiplied by the height it is to be discharged, multiplied by the pump capacity.
 Expressed mathematically: (8.58 lb/min) (100 gal/min) (15 ft) = 12,870 foot-pounds
 Using the conversion factor of: 33,000 foot pounds per minute = 1 horsepower. The theoretical HP required to operate the pump would be: 12,870 foot-pounds per min ÷ 33,000 foot-pounds per min per HP = 0.390 HP
 The mechanical efficiency of the pump is 92.5 %, so actual HP required to operate the pump would be: **0.390 HP ÷ 0.925 (mechanical efficiency) = 0.421 HP = Minimum HP of motor required to effectively operate the pump.**
- C. ¾ HP **Incorrect Answer:** The ¾ HP (0.750 HP) motor could operate the pump, but is not the smallest HP motor available to operate the pump.
- D. 1.0 HP **Incorrect Answer:** The 1.0 HP motor could operate the pump, but is not the smallest HP motor available to operate the pump.
-
4. A. air ejector inter-condenser **Correct Answer:** Condensate discharged by the main condensate pump first passes through the tubes of the air ejector inter-condenser. The condensate passing through the inter-condenser tubes condenses the steam/gas mixture discharged to the inter-condenser shell by the first stage air ejector unit. The resultant condensate drops to the bottom of the inter-condenser shell, and drains back to the main condenser via a U-shaped loop seal.
- B. main condenser hotwell **Incorrect Answer:** The main condensate pump takes suction from the main condenser hot-well.
- C. air ejector after-condenser **Incorrect Answer:** Upon exiting the air ejector inter-condenser tubes, condensate from the main condensate pump then flows through the tubes of the air ejector after-condenser. The condensate passing through the after-condenser tubes condenses the steam/gas mixture discharged to the after-condenser shell by the second stage air ejector unit. The resultant condensate drops to the bottom of the after-condenser shell, and drains back to the atmospheric drain tank.
- D. DC heater vent condenser **Incorrect Answer:** Condensate discharged by the main condensate pump must pass through the air ejector condenser unit and gland exhaust condenser before entering the DC heater vent condenser.

Nautical Deck Queries

Prepared by NMC Deck Examination Team

Q

uestions

1. International & Inland: What describes a head-on situation?

- A. Seeing a vessel displaying both sidelights ONLY dead ahead.
- B. Seeing two forward white towing identification lights in a vertical line on a towing vessel directly ahead.
- C. Seeing both sidelights of a vessel directly off your starboard beam.
- D. Seeing both sidelights and masthead light(s) of a vessel dead ahead.

2. What is the computed breaking strength of a 4-inch manila line?

- A. 5,280 lbs.
- B. 7,700 lbs.
- C. 12,200 lbs.
- D. 14,400 lbs.

3. You are loading a cargo that includes cylinders of acetylene aboard your break bulk vessel. Which statement is true?

- A. The cylinders must be stowed at least 10 horizontal feet from corrosive materials in the same space.
- B. Stowage in the upper deck is considered to be the equivalent of "on deck" stowage for this cargo.
- C. The cylinders must have a red label for flammability and a green label for compressed gas.
- D. The cylinders may be protected from the radiant heat of the sun by laying a tarp on them.

4. You are bound for Baltimore via Cape Henry on a 15 knot ship. If the flood at Chesapeake Bay entrance begins at 1800 EST (ZD +5), at what time would you depart from the Chesapeake Bay entrance to have the most favorable current?

- A. 1700 hours
- B. 1800 hours
- C. 1900 hours
- D. 2030 hours

1. A. Seeing a vessel displaying both sidelights ONLY dead ahead. Incorrect answer.
- B. Seeing two forward white towing identification lights in a vertical line on a towing vessel directly ahead. Incorrect answer.
- C. Seeing both sidelights of a vessel directly off your starboard beam. Incorrect answer.
- D. Seeing both sidelights and masthead light(s) of a vessel dead ahead. **Correct answer.** Rule 14: Defines a head on situation when two power-driven vessels are meeting on a reciprocal or nearly reciprocal course. Such a situation is deemed to exist when a vessel sees the other ahead or nearly ahead and by night she could see the masthead lights of the other in a line and/or both sidelights and by day she observes the corresponding aspect of the other vessel.

2. A. 5,280 lbs. Incorrect answer.
- B. 7,700 lbs. Incorrect answer.
- C. 12,200 lbs. Incorrect answer.
- D. 14,400 lbs. **Correct answer.** Manila line is measure by circumference, $C=4$ inches. Breaking strength in long tons is computed by the formula $BS=C^2/2.5$.
 $(4^2)/2.5=6.4$ long tons.
 1 long ton is equal to 2,240 lbs.
 6.4 long tons \times 2,240 lbs. = 14,336 lbs.

3. A. The cylinders must be stowed at least 10 horizontal feet from corrosive materials in the same space. **Correct answer.** 49 CFR 176.83(b)—General Segregation Requirements for Hazardous Materials tells us cylinders of acetylene, a class 2.1 Flammable gas and class 8 corrosive materials, should be kept “away from” each other. 49 CFR 176.83(c)2(i)C(ii) defines “Away from” as effectively segregated so that the incompatible materials cannot interact dangerously in the event of an accident but may be carried in the same compartment or hold or on deck provided a minimum horizontal separation of 3 m (10 feet) projected vertically is obtained.
- B. Stowage in the upper deck is considered to be the equivalent of “on deck” stowage for this cargo. Incorrect answer.
- C. The cylinders must have a red label for flammability and a green label for compressed gas. Incorrect answer.
- D. The cylinders may be protected from the radiant heat of the sun by laying a tarp on them. Incorrect answer.

4. A. 1700 hours Incorrect answer.
- B. 1800 hours Incorrect answer.
- C. 1900 hours Incorrect answer.
- D. 2030 hours **Correct answer:** The following information is referenced from COMDTPUB P16721.46 Reprints from the tide tables and tidal current tables, which is available in the exam room:

Currents are cyclical; there are two ebbs and two floods occurring within every 24 hour period. There is a slack water period between each maximum ebb or flood. Using this information we know that approximately every six hours the direction of the current changes and approximately every three hours there is a slack water period.

Comparisons of predicted with observed times of slack water indicate that more than 90 percent of the slack waters occurred within half an hour of the predicted times. To make sure, therefore, of getting the full advantage of a favorable current or slack water, the navigator should reach the entrance or straight at least a half hour before the predicted time of the desired condition of current.

The question tells us that flood at Chesapeake Bay entrance is at 1800. The current table tells us that slack water is the most favorable state of the current. If flood is at 1800 we can reasonably surmise the next slack will be at approximately 2100 or three hours later. The current table tells us we should arrive at the Chesapeake Bay entrance one half hour prior to that time or at 2030 hours.

Upcoming in

- **Combating Piracy**
- **100 Years of Marine Safety**
- **Marine Casualty Investigation Process**
- **The Arctic**

If your command is interested in "Championing" a *Proceedings* edition, contact the executive editor at 202-372-2315. Champion's Guidelines are available on the *Proceedings* website, www.uscg.mil/proceedings.

Mailing Address:
U.S. Coast Guard,
Proceedings Magazine,
2100 2nd St. S.W.
Mail Stop 7681
Washington, DC 20593

Phone:
202-372-2316

Email:
HQS-DG-NMCPROCEEDINGS@USCG.MIL

Website:
www.uscg.mil/proceedings

**COMMANDANT (DCO-84)
ATTN PROCEEDINGS
US COAST GUARD
2100 2ND STREET SW STOP 7681
WASHINGTON DC 20593-7681**

PRSRT STD
POSTAGE & FEES PAID
U.S. COAST GUARD
PERMIT NO.G-157

Official Business
Penalty for Private Use, \$300

FORWARDING SERVICE REQUESTED

