Waves on the Waterfront

CG-FAC, Office of Port and Facility Compliance

Safety, Security, and Stewardship

Volume 4
Issue 4

August 2015

SPECIAL ANNOUNCEMENTS

Next NMSAC Meeting

The Next Public meeting of the National Maritime Security Advisory Committee will be held September 29-30 in Washington, DC.

Topics will include: The CG Cyber Strategy, TWIC Next Generation readers, and CG Industry Training Program Revisions. The meeting will be broadcast via webinar at: https://share.dhs.gov/nmsac/

Bennis Award

September will start the solicitation period for the 2015-2016 Rear Admiral Richard E. Bennis Award Applications. Stay Tuned for more details.

Feedback

We welcome any suggestions! Please submit comments to Mr. Ryan Owens at: Ryan.F.Owens@uscg.mil.

Cyber Security and Cyber Risk Management

Cyber problems are increasingly in the news these days, with attacks on government and private sector organizations alike. The Coast Guard recently published our Cyber Strategy, see page 7, that outlines our approach. This edition of Waves on the Waterfront is largely devoted to cyber issues.

Note that the Coast Guard has a Cyber Strategy, not a "cyber security" strategy. Cyber certainly has a significant security aspect, with nation states, terrorists, and trans national organized crime networks as significant threats. However, cyber also has a safety aspect, in which accidental events, such as non-targeted malware finding its way onto vital systems, or simple technical problems such as failed software updates can lead to serious consequences.

From both a safety and a security perspective, sound risk management principles combined with basic cyber procedures can substantially reduce risk. For more on this, read the article from VADM Michel, RDML Thomas, and Yours Truly.

CG-FAC is leading the Coast Guard's effort to develop cyber risk management guidelines for the marine industry, and to provide training and other resources to Coast Guard facility inspectors and other personnel working with the industry.

As always, Coast Guard field units are not waiting on Headquarters, and I appreciate the great work done through Area Maritime Security Committees, and others, to address cyber risks. That work is informing our efforts and making cyber part of our overall critical infrastructure protection program.

Keep (cyber) safe

Captain Andrew Tucci, CG-FAC

QUESTIONS FROM THE FIELD

There has been a slew of news reports about a cyber security incidents that have impacted the data of federal government employees, contractors, and others. A number of Coast Guard field units and industry personnel have asked CG-FAC if these events have any nexus to Coast Guard systems, such as Homeport and TWIC. Full details can be found at https://www.opm.gov/cybersecurity, but here are some common questions:

Question 1. "What data was impacted?"

Answer: In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security Numbers were affected. This number has not changed since it was announced by OPM in early June and you should have already received a notification if you were impacted.

While investigating this incident, in early June 2015, OPM discovered that additional information had been compromised: including background investigation records of current, former, and prospective Federal employees and contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

The Types of information involved in the background investigation records incident that may have been impacted:

- Social Security Numbers
- Residency and educational history
- Employment history
- Information about immediate family and personal and business acquaintances
- Health, criminal and financial history that would have been provided as part of your background investigation

Question 3: I have a TWIC card, was my data compromised?

Answer: No, The TWIC database was not impacted.

Question 4: I have a clearance through the Coast Guard's Stale, Local, and Industry clearance program. Was my data compromised?

Answer: Most likely. If you underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P for a new investigation or periodic reinvestigation), it is highly likely that you are impacted by this cyber incident. If you underwent a background investigation prior to 2000, you still may be impacted, but it is less likely.

Cyber Risks in the Maritime Transportation System

Vice Admiral Charles D. Michel, Rear Admiral Paul F. Thomas, and Captain Andrew Tucci

Historic Background and Coast Guard Mission

The U.S. Coast Guard has a long history of protecting our nation from all manner of threats and hazards. When Alexander Hamilton founded what was then called the Revenue Marine, he charged those early sailors with patrolling our coasts and protecting our ports with vigilance.

Piracy and smuggling were the main threats of the day, but soon enough other risks appeared. Boiler explosions, navigation hazards, and fires on merchant vessels all threatened the safety of the nation's marine transportation system. The Coast Guard, including our various predecessor agencies, developed the capabilities needed to protect the nation from those and other risks, including oil spills, the dominance of foreign flag ships for our overseas trade, and terrorism. Stemming from the sabotage at Black Tom's Island in New York in 1916, the Coast Guard established Captains of the Port whose duties center on port wide risks and maritime critical infrastructure protection.

Today, cyber related risks are unquestionably a large and rapidly growing portion of all the risks our ports, facilities, and vessels face. The Coast Guard must address this threat if we are going to continue to achieve our mission of protecting the safety, security, and stewardship of America's waters.

Cyber Risks and the Marine Transportation System

The U.S. Coast Guard is proud of our service to the country. We are also grateful for the professionalism and cooperation of the marine industry in helping to build and operate the safest, most secure Marine Transportation System (MTS) in the world. The ports, terminals, vessels, related infrastructure and, most importantly the people that operate it drive the American economy and are vital to the nation's strength and prosperity.

Vessel and facility operators use computers and cyber dependent technologies for navigation, communications, engineering, cargo, ballast, safety, environmental control, and many other purposes. Emergency systems such as security monitoring, fire detection, and alarms increasingly rely on cyber technology. Collectively these technologies enable the MTS to operate with an impressive record of efficiency and reliability.

The Coast Guard's mission is to reduce the risk of deaths, injuries, property damage, environmental impacts, and disruptions to the MTS itself. Accordingly, our focus is on industrial control and other systems that could lead to these types of events. The integrity of IT systems that handle, for example, financial transactions is not, *per se*, a Coast Guard concern. Sound cyber risk programs will look at all types of risk, and operators need to be alert for the possibility that low risk or administrative IT systems may provide a network connection or backdoor to higher risk systems.

While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, or disrupt vital trade activity. For example, vessels rely almost exclusively on networked GPS-based systems for navigation, while facilities often use the same technologies for cargo tracking and control. Each provides multiple sources of failure, either through a disruption to the GPS signal, or malware that impacts the way the signal is interpreted, displayed, and used on the vessel or facility.

Cyber vulnerabilities are in no way limited to GPS. Engineering and other systems are equally vulnerable. The Coast Guard and other authorities have documented cyber related impacts on technologies ranging from container terminal operations ashore to offshore platform stability and dynamic positioning systems for offshore supply vessels. While in some cases modern day pirates and smugglers have been the source of these events, others have been the result of non-targeted malware or relatively unsophisticated insider threats Even legitimate functions, such as remotely driven software updates, could disable vital systems if done at the wrong time or under the wrong conditions.

The engine control room on a modern cruise ship. Photo credit: LCDR Eric Allen, USCG

Commercial pressure and the ever increasing demand for speed, efficiency, centralized control, and convenience creates incentives to make greater and more integrated use of these systems. This in turn increases vulnerability and the "attack surface" available to hackers and criminals, as well as to simple misuse.

Vessel and facility operators must be able to recognize cyber risks alongside more conventional threats and vulnerabilities. Once recognized, operators should address them via established safety and security regimens, such as security plans, safety management systems, and company policies.

The U.S. Coast Guard Strategic Approach

The Coast Guard's operating model for all types of risk is to prevent incidents, accidents, and attacks whenever possible, and to be prepared to respond to those events when they do occur. Both have a role in the Coast Guard's Cyber Strategy. The Prevention side of this equation is to identify and establish broadly accepted industry standards that reduce the likelihood of an incident occurring. In developing Prevention standards and programs for cyber and other vulnerabilities, the following principles apply:

The Coast Guard's Prevention Program:

Risk Based,

Performance Oriented,

Customized to the marine environment

Principles of the Coast Guard's Prevention Program

The Coast Guard's prevention standards are ***risk based***. That is, they correlate the degree of protection with the potential consequences. For example, vessels and facilities that handle liquefied natural gas are subject to greater requirements than those that handle most other products. For any individual vessel or facility, vital systems such as firefighting, lifesaving, and communications are generally given more scrutiny than those with only a secondary influence on safety or security.

In addressing potential cyber vulnerabilities, the Coast Guard will follow a similar risk based approach. While a vessel or facility may have any number of cyber dependent systems, our concern is with those few where failure or exploitation of the system might result in significant safety, security, or environmental consequences.

A second principle is that the Coast Guard uses ***performance standards*** wherever possible. That is, the purpose of our standards is to achieve a high degree of safety and security performance – to protect the mariners, facility workers and vessel passengers from harm, to protect the marine environment, and to avoid damage to property and equipment. There are many ways to accomplish that goal, and the Coast Guard strives to allow industry the greatest flexibility. In some cases, such as with our Maritime Transportation Security Act requirements, our regulations are almost entirely performance based. Even in cases where more prescriptive requirements are appropriate, such as engineering standards, the Coast Guard allows and encourages industry to propose alternative methods that achieve an equivalent level of safety or security.

Coast Guard personnel observing the security and safety control systems at a marine terminal. USCG photo

Despite the technical nature of cyber systems, the Coast Guard believes that the principle of performance standards can and should be part of any vessel or facility's approach to reducing cyber risks. In some cases, an operator may choose to mitigate a cyber vulnerability through an established technical protocol. In other cases, training programs, physical access controls, or a simple manual backup may be a better option. The business needs of the organization should serve to identify the best method of reducing the risk.

Cyber risks are an international threat. The Coast Guard is working with the International Maritime Organization to improve cyber risk management for vessels and ports subject to SOLAS and the ISPS Code

IMO

A third aspect of the Coast Guard's Prevention model is that our standards reflect the ***unique risks of the marine environment***. Heat, vibration, salt water, weather, and other factors require standards suitable for this environment. Coast Guard approval of items such as fire extinguishers and marine wiring reflect this reality.

The marine environment includes unique risks that any cyber risk management effort must address. These include serious consequences to people, the environment, property, and the marine transportation system as a whole. The Coast Guard's cyber risk management program is concerned with these special maritime risks. Businesses certainly face other cyber risks, such as the loss of proprietary or financial data. These risks, while very real, are not unique to the maritime environment and are outside the Coast Guard's mission. The technical aspects of cyber security are also not uniquely maritime. Computers onboard a vessel or on a marine facility are no different from those in other environments, and the threats they face come in one and zeros wherever the computer is located and without regard to its ultimate function. Technical protocols need to be appropriate for the system and threat in question. They need no modification for vessel or marine facility use.

Response, Investigation and Recovery

Because we can't expect to prevent all incidents (cyber related or otherwise), preparedness is equally important to reducing the overall risk to the public and MTS. In many cases, addressing the consequences of a cyber event – such as an oil spill caused by computer controlled pump – is no different than if the incident had no cyber aspect. In such an incident, the responsible party would activate their spill response plan under the direction of the Coast Guard and other agency officials.

The Coast Guard investigates pollution incidents, marine casualties and certain other incidents to determine the factors that led to the incident and prevent reoccurrences. If the investigation reveals a cyber nexus, the Coast Guard will work with law enforcement and other appropriate agencies to gather evidence and support criminal prosecution. In all cases, the Coast Guard will typically require the operator to conduct tests or inspections to ensure a system is safe before resuming normal operations. For cyber incidents, that process might include measures to ensure a system is free of malware or known vulnerabilities.

The NIST Framework identifies the following core functions:

Identify
Protect
Detect
Respond
Recover

How Can Vessel and Facility Operators Manage Cyber Risks?

The marine industry has a long history of success in risk management. Mariners and port workers identify and evaluate risks on every watch and shift. Vessel and facility operators should view cyber along with the physical, human factor, and other risks they already face. The NIST Framework provides guidance on how to accomplish this. The first step is to identify and evaluate the sources of risk.

While physical and personnel risks are relatively easy to identify, cyber risks pose a unique challenge. Cyber vulnerabilities are invisible to the casual observer and cyber attacks can originate from anywhere in the world. Information technology specialists can help, but their focus is often with routine business applications. IT specialists may not fully recognize the various operational systems on a vessel or waterfront, the potential consequences should they fail, or have an operator's perspective on potential non-technical (and lower cost) solutions.

Risk Assessment:

To assess cyber risk, designate a responsible individual and assemble a team that includes operators, emergency managers, safety, security, and information technology specialists. Very briefly, their risk assessment process would proceed as follows:

- Inventory cyber dependent systems that perform or support vital operational, safety, security, or environmental protection functions.
- Map any connections between these systems and other networks. Note which systems are accessible via routine internet connection and for portable media such as USB and CD drives. This step in the process helps to identify potential **vulnerabilities**. Note that even systems with no connection to the internet whatsoever are still subject to insider threats and simple technical failures.
- For each system, discuss the potential **consequences** if the system was exploited, malfunctioned, was unavailable, or simply failed under "worst case scenario" situations. Remember, Murphy's Law always applies, and adversaries may combine a cyber attack with a physical attack.

There are many private and public resources available to help companies address cyber risks, including ICS-CERT. Identifying these resources in advance and designating specific personnel with the responsibility to contact them will improve preparedness.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Risk Mitigation:

Once the team recognizes their cyber risks, the organization can select mitigation strategies to reduce that risk. Prevention/protection strategies reduce vulnerabilities and the frequency of successful attacks or adverse events. While high-risk systems should naturally have more robust protection strategies, this does not necessarily equate to sophisticated technical solutions. For example, physical access control and training may be sufficient for systems where the primary vulnerability is an insider threat. Where risk managers choose technical solutions, they must also recognize their limitations.

Many systems are only capable of recognizing and blocking known threats. Unfortunately, the pace of innovation in the malware world is increasing, zero day exploits are common, and a strategy that relies exclusively on a perimeter defense designed to filter out known threats will not be successful.

Operators can also reduce risk at the consequence end. For example, manual backups may be appropriate for situations where the cyber failure is disruptive, but does not include immediate life, safety, or environmental impacts. Manual backups can be an excellent way of building cyber resilience – provided the manual system is reliable and personnel still know how to use it!

Exercises can help identify the procedures an organization may need to take to isolate a suspect system, purge it of malware, and safely resume operations. Including a cyber aspect into an existing security, natural disaster, or environmental response plan can help an organization prepare for a cyber incident with an "all hazards" approach.

The term *Defense in Depth* refers to a multi-faceted and multilayered approach to cyber defense.

Defense in depth considers the various people, technology, and operating policies an organization might adopt. It includes protection, detection, response, and recovery activities. Defense in depth recognizes that no single strategy can ensure security.

The teamwork approach among operators, IT specialists, and other risk managers is vital. Only a multi-talented team can develop multi-talented solutions. Regardless of the strategy chosen, operators need to see risk assessment and risk mitigation as continuous processes, not one-time- events. While this is true for any risk an organization may face, the rapid change in technology and its ever increasing use in society make this especially important.

Risk Management:

Once an organization has identified, evaluated, and mitigated cyber related risks to an acceptable level, it must still do two things to maintain that condition. First, organizations need to incorporate their cyber procedures into appropriate internal policy and operating requirements. These will vary from organization to organization, but may include the following:

- Safety Management System/ISO procedures
- MTSA required security plans
- Operations manuals
- Continuity of Operations/Continuity of Business plans
- Company training programs and policies

Second, because no risk is static, organizations must view cyber security as a process, and establish a regular schedule to review cyber risks, re-evaluate the need for mitigation measures, and ensure personnel understand and can follow good cyber practices. Rapid changes in technology and ubiquitous cyber threats make this concept especially important. Ultimately, an organization should strive to incorporate cyber into an existing culture of safety, security, and risk management.

Ultimately, cyber risk management is a leadership responsibility. Organizations should identify a senior individual as the person responsible for cyber risk management. That individual, and other leaders, must recognize that creating a strong cyber culture as an “all hands” responsibility. With the visible backing of senior leadership, an organization can develop the strong cyber culture needed to keep the operations safe, secure, and efficient.

Conclusion:

Despite the apparent complexity and scale of cyber threats, we can and are adding cyber to a long list of risks the maritime industry and the Coast Guard have overcome. More senior members of the Coast Guard, and of industry can look back on their careers and see great advances in environmental stewardship, safety, and conventional security. Those accomplishments reflect a cooperative approach that establishes meaningful standards to address real risks, devises flexible strategies to meet those standards, and shares responsibilities to maintain those systems over time. We have strengthened our nation and ensured that our ports and waterways are a safe place to live, conduct business, and link our economy to the world.

While cyber risk management certainly requires some technical skills from the current and next generation of leaders, it will succeed on the foundation of those of us (these authors included) that still think an A-60 bulkhead is the best firewall for any situation.

Appendix – Cybersecurity Roles and Responsibilities

A full discussion of the various cyber security related authorities and responsibilities within the federal government is beyond the scope of this paper. Broadly speaking, the Department of Homeland Security is primarily responsible for critical infrastructure protection, the Department of Justice is primarily responsible for criminal investigations, while the Department of Defense is responsible for national defense.

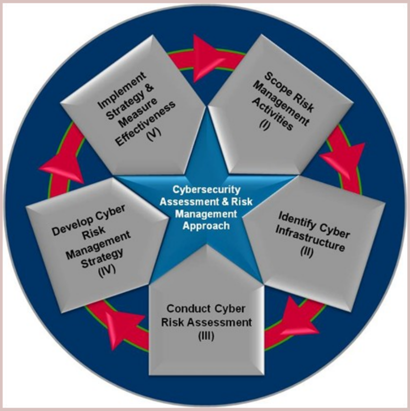
	DHS	**DOJ**	**DOD**
Lead role	**Protection, Information Sharing**	**Investigation and Prosecution**	**National Defense**
Responsibilities	Coordinate national response to significant cyber incidents Disseminate domestic cyber threat and vulnerability analysis Protect critical infrastructure Secure federal civilian systems Investigate cyber crimes under DHS jurisdiction Coordinate cyber threat investigations	Prosecute cyber crimes Investigate cyber crimes Lead domestic national security operations Conduct domestic collection and analysis of cyber threat intelligence Coordinate cyber threat investigations	Defend the nation from attack Gather foreign cyber threat intelligence Secure national security and military systems Support the national protection, prevention, mitigation of, and recovery from cyber incidents Investigate cyber crimes under military jurisdiction

The U.S. Coast Guard, as a member of the Department of Homeland Security, has responsibility to help protect the nation’s maritime critical infrastructure, and to promote safety and security in the Marine Transportation System. As a member of the U.S. Armed Forces, the Coast Guard works closely with the Department of Defense, including U.S. Cyber Command, in defending the nation. As a law enforcement agency, the Coast Guard has authority to investigate violations of all federal crimes with a maritime nexus (14 U.S.C.). Finally, the Coast Guard is a member of the intelligence community, providing us access to many sources of information that can help us with our mission to protect the American people.

Cybersecurity Assessment and Risk Management Approach (CARMA)

By LCDR Josh Rose

The week of June 8th, a whole host of federal agencies, along with industry port stakeholders came together at Sector Del Bay in Philadelphia, Pennsylvania to tackle cyber risk management. DHS Office of Sector Engagement Critical Infrastructure Resilience, in conjunction with the Coast Guard, led a cyber risk assessment in the COTP Delaware Bay. This was a great example of federal agencies and Port Stakeholders coming together to try and assess cyber risk within a port. Along with DHS, other federal agencies present included National Institute of Standards and Technology (NIST), Federal Energy Regulatory Commission (FERC), Customs and Border Protection (CBP), and the Transportation Security Administration (TSA). From the Coast Guard, along with members from Sector Del Bay, D5, LANTAREA, CG-FAC, CG-CVC and industry port stakeholders were represented. Two assessments completed were Cybersecurity Assessment and Risk Management Approach and Cybersecurity Resiliency Review.


Cybersecurity Assessment & Risk Management Approach
Scope Risk Management Activities (I)
Identify Cyber Infrastructure (II)
Conduct Cyber Risk Assessment (III)
Develop Cyber Risk Management Strategy (IV)
Implement Strategy & Measure Effectiveness (V)

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

Cybersecurity Resiliency Review (CRR) is a review of the overall practice, integration, and health of an organization's cybersecurity program. The CRR seeks to understand cyber security management of services (and associate assets) critical for an organization's mission success by focusing on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization. The difference between CARMA and CRR is that CARMA is a port-wide risk assessment while the CRR looks at the maturity of an individual organization's cyber resiliency. Three organizations volunteered to conduct the CRR once the CARMA assessment was complete.

What about the other agencies?

Each agency that attended was there to assist the Coast Guard with identifying how cyber systems are used and interconnected within the port environment. NIST is assisting in developing implementation guides for using the Cybersecurity Framework within the Maritime Transportation System. TSA, who chairs the Transportation Sector Specific Cybersecurity Working Group, observed how the port assessment not only affects the maritime environment, but also other modes of transportation operating within the port. FERC, who has already established cyber guidelines, offered their support and gave lessons learned

Continued on next page

(Continued from Page 5)

on obstacles they faced when developing standards for the energy sector. It was an excellent demonstration of federal agencies working together for a common goal.

What is next?

As with any new tool, there were many lessons learned in the week-long assessment. Understanding appropriate scale of the scenario given during the assessment and what additional industry stakeholders we should recruit are two lessons learned from the Philadelphia assessment. This office plans to continue collaboration with the government agencies in attendance to further the Coast Guard's implementation of the Cyber Strategy. Thanks to Sector Delaware Bay staff for their assistance with making this assessment such a success!

Cyber Security, What Can be Done.

The process of securing your cyber systems parallel in structure to that of other security and safety efforts: assess risk, adopt measures to reduce that risk, assess progress, revise, and continue. These processes, taken together, can significantly improve an organization's risk reduction efforts and increase resilience through continuity of business planning.

Looking specifically at cyber security, consider the following steps:

- Conduct a Risk Assessment – begin by assessing what parts of your enterprise are controlled or supported by computer systems. What are the consequences should those systems become inoperable, controlled by outside parties, or misused by internal parties?

- Identify and Adopt Best Practices – what information technology security standards are most applicable to your systems? Are your systems meeting those standards, are your employees familiar with them? When were they last updated? What backup systems, redundancies, or replacements are available?

- Secure Your Supply Chain – As with just-in-time inventory and production systems, consider the cyber vulnerabilities and practices of your suppliers, customers, and other organizations critical to your company's profitability. Discuss cyber security with those organizations and consider incorporating good cyber practices into marketing and contracting.

- Measure Your Progress – Test your cyber practices through drills and exercises. Identify any gaps or lessons learned, and set specific goals with timelines for making needed improvements.

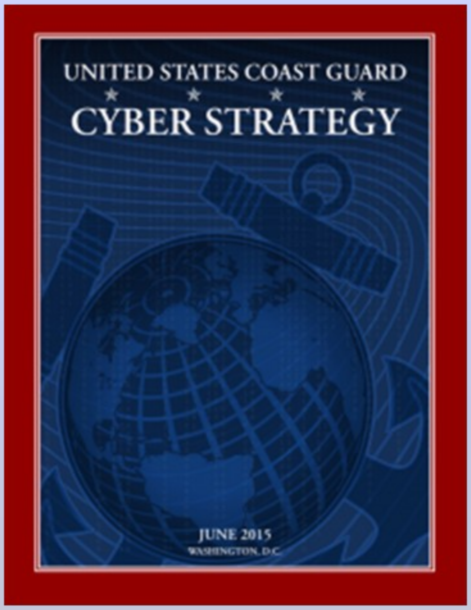
- Revise and improve security – Review your latest risk assessment, evaluate any new cyber systems you may have added since that time, incorporate lessons learned and revise your cyber security policies and procedures accordingly.

One way to start this process is to take advantage of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICSCERT). ICS-CERT provides a wide range of information, tools, and services that can help companies assess their security, identify recommended practices, and improve their cyber security. http://ics-cert.us-cert.gov/

New Tactics, Techniques, and Procedures (TTPs) Available

The Office of Waterways Management (CG-WWM) is pleased to announce that two Tactics, Techniques, and Procedures (TTPs) were signed on July 31, 2015 and ready and available for use. These TTPS address the administrative and other functions associated with issuing COTP Orders, and with Anchorage Management. They are intended for Coast Guard Waterway Management and other personnel in addressing various Captain of the Port and Waterway Management Functions. They are located on the CG Portal (intranet) at https://cg.portal.uscg.mil/communities/hp/HPCenter/TTP/Default.aspx

These TTPs represent a significant milestone and important step in helping sector staff learn, train, and execute COTP Orders with greater effectiveness and efficiency. These TTPs will also help FORCECOM to tailor course curriculums and Assessments, Inspections, and Audits (AIA) to align with the best practices in the field today.



UNITED STATES COAST GUARD

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

Coast Guard Cyber Strategy

by LT Josephine Long and Myra Gerald

For more than two centuries, the U.S. Coast Guard has harnessed innovations and leveraged new capabilities to ensure safety, security and stewardship across the maritime domain. In continuing a proud history of responding to the nation's maritime needs, the Coast Guard has fully embraced a new operating domain – cyberspace. On June 16th the Commandant released his new Cyber Strategy, which aligns with the Department of Homeland Security's and Department of Defense's plans and will guide the service's efforts in the cyber domain for the next 10 years.

The Coast Guard Cyber Strategy identifies three distinct strategic priorities crucial to the service's mission: defending cyberspace, enabling operations and protecting infrastructure. In all of these efforts our goal is a common one: identify and address cyber risks to the maritime domain.

Protecting Infrastructure, the third priority of the strategy has two goals: promote cyber risk awareness and management and reduce cybersecurity vulnerabilities in the marine transportation system. The maritime transportation system, and its associated infrastructure, is vital to America's economy, security and defense. While cyber systems enable the maritime transportation system to operate with unprecedented speed and efficiency, those same systems also create potential vulnerabilities.

By employing its new cyber strategy, the Coast Guard will work tirelessly to achieve our vision for operating in the cyber domain: We will ensure the security of our cyberspace, maintain superiority over our adversaries and safeguard our Nation's critical maritime infrastructure.

A digital copy of the Cyber Strategy can be found at http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf

SAFETY FIRST!

5 GAS METERS

Coast Guard facility inspectors spend much of their time climbing around cargo manifolds, hoses, pipes, and venting systems that handle hazardous materials. When these systems are properly maintained, and operating under normal conditions, they should not present any atmospheric hazards to Coast Guard or industry personnel. That said, we all know there are times when conditions are not ideal, and where hazards may exist.

The best way to protect yourself from potential atmospheric hazards is to begin every operations with an operational risk management assessment. Safety is a leadership responsibility. The team leader should discuss the possible risks of the activity with other team members, identify possible hazards, and ensure that all members employ the right procedures and personnel protective equipment to minimize risk. A discussion with the facility person in charge, vessel master, or terminal operator about any unusual conditions, and company safety policies, should be part of this assessment.

CG-FAC, in cooperation with CG-113, is purchasing and distributing 5 gas meters to Coast Guard Sectors and MSUs. These meters enable field personnel to detect and measure the concentration of 5 atmospheric hazards commonly found at marine facilities, on barges and vessels, and during the course of marine environmental response operations.

Five gas meters and other instrumentation allow field personnel to verify that conditions are safe for routine operations. They also provide warning for hazards that may be difficult to detect or anticipate despite the best Operational Risk Management practices. Do not use them to justify entrance into a space or location where ORM would suggest that hazardous conditions are likely. In other words, if you expect the alarms to go off, stay out of the area or space!

Units should expect to receive their meters in September. An operational risk management job aid and other safety information is available at http://www.uscg.mil/hq/cg5/cg544/Safety.asp.

Office of Port and Facilities Compliance

Contact List

Office Chief

Captain Andrew Tucci	202 372-1080

Domestic Ports (CG-FAC-1)

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

Port Resiliency/Recovery Branch

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

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

LCDR Josh Rose	202-372-1106
LT Josephine Long	202-372-1109
Mr. Geoff White	202-372-1141
Mr. Robert Reimann	202-372-1146

Cargo and Facilities (CG-FAC-2)

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

Facility Safety (explosive handling, containers, COAs)

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

Facility Security (MTSA)

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

TWIC Implementation

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

Security Standards (Regulation Development)

LCDR Kevin McDonald	202-372-1168
LT Cal Fless	202-372-1123

USCG TWIC Help Desk

USCG TWIC Help Desk	202-372-1139 TWIC.HQ@uscg.mil

CG-FAC Links

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