NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
April 2017

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This news letter will be e-mailed to members of the Northern California Area Maritime Security Committee, posted on the Coast Guard's HOMEPORT portal and may be posted by the San Francisco Marine Exchange.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **Shipping Industry Vulnerable to Cyber-Attacks and GPS Jamming** – discusses the cybersecurity issues surrounding the shipping industrys increased reliance on computers and other information technoligies.
- **Maritime Cyber Security: on Whose Radar?** – discusses United States and International efforts to address cybersecuirty.
- **Hacked: Energy Industry's Controls Provide an Alluring Target for Cyber-attacks** – discusses issues surrounding the hacking of Industrial Control Systems (ICS).
- **S-133 Cybersecurity Bill Introduced** – a bill introduced into the U.S. Senate, authorizing the intelligence community to provide assistance to critical infrastructures/key assets and users of industrial control systems.
- **Common Sense Operational Security** – a discussion of common sense Operatinal Security (OPSEC) that everyone should take.
- **Keeping Your Network Secure** – a U.S. Government pamphlet about cybersecurity at home, expecially for persons that work from home.

- **Suspicious Activity & Breach of Security Reporting USCG Policy Letter** – a USCG Policy Letter dated December 14, 2016; that describes suspicious activities and breaches of security.

MAIN ARTICLES

Shipping Industry Vulnerable to Cyber-Attacks and GPS Jamming, February 1, 2017, Luke Gram (CNBC)

The shipping industry is increasingly at risk from cybersecurity attacks and a gap in insurance policies is leaving them vulnerable, industry experts have told CNBC. Cybersecurity has come into focus across the economy, as hackers become more capable. Meanwhile, ships are more reliant on a range of electronic devices to operate.

> "This includes software to run the engines, complex cargo management systems, automatic identification systems (AIS), global positioning systems (GPS) and electronic chart displays and information systems (ECDIS)," explained Matthew Montgomery, senior associate at international law firm Holman Fenwick Willan, told CNBC via email. "The added incentive for a hacker is that the shipping industry involves high value assets and the movement of valuable cargo on a daily basis."

Jamming or disrupting GPS systems creates significant problems. For example, in April last year, South Korea said that around 280 vessels had to return to port after experiencing problems with their navigation systems, and claimed North Korea was behind the disruption. Professor David Last, strategic advisor to the U.K.'s General Lighthouse Authorities which provides navigation aids for ships, recently ran a series of trials to examine the effect of GPS jamming on shipping. In one trial, a jammer was operated from a lighthouse and aimed at ships.

> "The effect was profound. It strongly affected GPS receivers on ships out to sea to the horizon at about 30km," he told CNBC during a phone call. "Some GPS receivers simply died. They wouldn't provide any information. But interestingly other ships' GPS receivers lied. That is to say they gave false positions. So, we had ships that were actually in the sea that appeared to be travelling over land."

A second series of trials placed a jammer on a ship, which caused multiple systems to fail, including navigation systems, emergency systems, the clocks and the automatic identification system, which transmits a ship's location to other nearby ships so they appear on radar.

> "We had ships that were in wrong positions and ships that suddenly began to move very gently without anybody realizing it," explained Last. Losing these systems can become a

> big problem when visibility is an issue and on busy shipping routes such as the English Channel. "When the weather is bad, when fog is down the visibility is low, they (the ships) depend entirely on GPS for their navigation," he said. "If GPS goes wrong, the potential for accidents is very high."

Another cause for concern is the fact many shipping companies may be uninsured in the event of a cyber-attack.

> "Most insurance policies covering ships include a cyber-attack exclusion clause which excludes cover for property damage and business interruption. This has left a potential exposure for ship owners," said Montgomery. According to Montgomery, the insurance market is responding to these gaps and starting to offer products which cover cybersecurity, but the shipping industry needs to identify which risks need to be insured and how to mitigate them. "Some ship owners are now identifying the areas where they are exposed to cyber risks, developing and testing written information security and incident response plans, and putting their incident response team through simulated exercises (with the assistance of external legal advisors) to see where the gaps are," he said. "Once a ship owner has implemented active cyber risk identification and mitigation processes, they are likely to be in the best possible position to transfer any remaining exposures through a cyber insurance policy."

Maritime Cyber Security: on Whose Radar? February 03, 2017, Sally Daultrey (OpenLens)

Glance through the headlines on any given day and it's easy to conclude that cyber security is mostly a city problem—high densities of people and their data create a virtual environment that's rich with opportunity for criminals seeking to exploit financial systems and the Internet of Things. On the high seas, in the world's ports and at the margins of every coastline, cyber security in the maritime domain is just as complex. Fixed and mobile assets cross multiple zones of jurisdiction and territory. Legacy infrastructures and communications systems with poor or no encryption are open to attack. With 90% of the world's cargo transiting by sea, there's a huge part of the global economy that we don't regularly "see" but is vital to the national critical infrastructure of most countries.

Cyber security incidents in the maritime sector, as on land, include deliberate attacks on infrastructure and vessels, accidental security breaches, and exploits. The total attack surface can be viewed in terms of mobile assets (vessels, containers, offshore oil and gas platforms, unmanned undersea vehicles, drones), fixed assets (port infrastructure, navigation aids, undersea cables and pipelines), and communications systems (onshore, ship-to-shore, and satellite). Ship-to-shore communications and port industrial control systems (ICS) are particularly vulnerable;

with no in-built signal encryption or authentication, AIS is a soft target (a feature that is exploited in the industry to transmit false location data). The data holdings of shipping firms and their service providers are a rich source of operational and financial information, crew and passenger data, and location and asset capabilities. Advances in unmanned vessels, drones, and remotely controlled systems increase the number of connected assets. The total cost of cyber-attacks in the maritime sector is unknown, but annual costs to the oil and gas sector are indicative.

In the past year, the maritime sector has conspicuously picked up the pace in the cyber security challenge. 2016 saw guidelines from the IMO (MSC.1/Circ. 1526), BIMCO, Lloyd's Register, and the US Coast Guard (among others). Conferences dedicated to maritime cyber security are well attended by the world's navies, CIOs, and lawyers—for example, NATO's first conference on maritime cyber security in October 2016 and the first major maritime cyber security conference in the US in March 2015. Shipping companies, offshore operators, and transportation companies are advised to adopt a cyber risk management approach, such as that advocated by the USCG.

Cyber security in the maritime domain is currently considered in the national security strategies of the UK and USA, among others, but strategy does not automatically generate solutions; maritime cyber, like other sectors, relies on a supply chain of risk managers, IT consultancies, and third-party providers all operating among flag states of varying security posture and quality. Companies and port authorities are advised to assess their particular circumstances. In the US, Executive Order 13636 (February 2013) concluded that the USCG has regulatory authority on cyber security. The US Bureau of Safety and Environmental Enforcement (BSEE) may soon follow, affecting offshore operators and all 360 ports around the US coastline. US legislation on maritime cyber security is likely to take form in 2017.

International laws and conventions on maritime cyber security are more challenging. ICS views international regulation as unnecessary. Security of crew, passengers, and vessels on the high seas has a long history of international convention and protocol, with 180 flag states assuming responsibility for the physical security of crew and vessels sailing under their name. In 2004, the International Maritime Organization (IMO) further amended SOLAS to include port and ship security, while IMO III (requiring audit of safety compliance) entered into force in 2016. However, as is also the case in the US, IMO relies on voluntary reporting of cyber security incidents from among its member states. Achieving a reasonable standard of cyber security in the maritime sector in as short a timeframe as possible calls upon an armada manned with expertise from: (i) critical infrastructure protection (particularly in the energy sector), (ii) supply chain risk analysis, and (iii) international law (particularly concerning UNCLOS).

Even acknowledging differences of opinion on the legal frameworks that enable freedom of navigation on the high seas, the founding principle is more than 400 years old and will likely hold good. The world's energy and cargo supply chains can't (yet) operate without it. Defending access to sea lanes is a jurisdictional minefield negotiated on dry land. But with rapidly advancing cyber capabilities offshore, the threat landscape has fundamentally changed.
In July 2016, NATO affirmed cyberspace as a domain of operations in which international law applies. Arguably, preemptive cyber-attack as an offensive defense strategy is already in play. It has yet to be tested at sea, but the opportunity may soon arise. Consider China's defense infrastructure on seven newly constructed artificial islands in the Bohai Sea—in firing range of one of the world's busiest sea lanes—and the response to the discovery of an underwater drone measuring salinity in the South China Seas. In a different kind of warfare, maritime security, among the oldest traditions of all nations that have prospered on the high seas, has entered a new era.

Hacked: Energy Industry's Controls Provide an Alluring Target for Cyber-attacks, March 6, 2017, Collin Eaton (Houston Chronicle)

A Coast Guard cutter glides along the waters of the Sabine-Neches waterway, conducting sweeps for unprotected wireless signals that hackers could use to gain access to oil, gas and petrochemical facilities. Four massive refineries sit along the 79-mile channel that cuts through this stretch of Gulf Coast. It's one of the largest concentration of refineries, pipelines, chemical plants and natural gas terminals in the United States - and an alluring target for espionage, disruption or worse.

> "There are actors that are scanning for these vulnerable systems and taking advantage of those weaknesses when they find them," said Marty Edwards, director of U.S. Homeland Security's Cyber Emergency Response Team for industrial systems.

As national attention focuses on Russian cyberattacks aimed at influencing the last presidential election, oil and gas companies face increasingly sophisticated hackers seeking to steal trade secrets and manipulate industrial sensors and operations. Nowhere is the threat more consequential than in Houston and Southeast Texas, where the world's most celebrated names in energy produce, refine and transport fossil fuels, including Exxon Mobil, Royal Dutch Shell and Phillips 66. The operation aboard the Coast Guard cutter, a joint effort with Houston Police last April, was one of the first of its kind in the U.S. to focus on cyberattacks by sea.

The U.S. Department of Homeland Security, responsible for protecting the nation from cybercrime, received reports of more than 350 incidents at energy companies between 2011 and 2015. In most cases, a hacker infiltrated or tried to infiltrate the control systems of energy firms. During that period, the agency identified nearly 900 security vulnerabilities within U.S. energy

companies, more than any other industry. The vastness of oil and gas operations makes it difficult to secure. Thousands of interconnected sensors and automated controls that run oil and gas facilities remain rife with weak spots. Much of this equipment was designed decades ago without security features. In recent years, companies have linked devices that monitor pressure, control valves and initiate safety procedures to computer networks and - sometimes inadvertently - the internet.

> Those connections expose refineries, pipelines and offshore oil platforms to online threats. "You could mess with a refinery or cause a vessel to explode," said Richard Garcia, a former FBI agent who became a cybersecurity specialist.

The Coast Guard has received several reports that foreign ships attempted to probe the wireless networks of industrial facilities along U.S. waterways, federal authorities say. Homeland Security, which oversees the Coast Guard, declined to confirm details of any operation and intelligence but acknowledged a growing effort to protect oil, gas and chemical systems from hacking. Many energy companies, however, lack the technology and personnel to detect whether hackers have broken into operational systems using sophisticated malware that can take over controls or extract data. In fact, many oil and gas facilities still use networks run by Windows XP, a 2003 system that Microsoft no longer updates, according to federal authorities and cyber security consultants. Others use even earlier versions of the Windows operating system from the 1990s; in rare cases, a few still use MS-DOS, the precursor to Windows.

> "More often than not," Edwards said, "we find that there's been corners cut or they haven't taken a hard look at security when they designed those networks."

'What we don't know'

Strict cybersecurity regulations govern power, chemical and nuclear facilities, but no federal laws impose such standards in the oil and gas industry. When oil and gas companies have been infiltrated by a hacker, they aren't required to report the incident. And if they turn to federal authorities for help, the specifics are typically kept secret because companies disclose information in exchange for anonymity and discretion. Homeland Security publishes data on cyberattacks, but with no reporting requirements, the data represent only a small share of the cyberattacks against the energy industry.

> "We only know what's reported to us," Edwards said. "We don't know what we don't know."

Most companies are loath to talk publicly about the security of computer systems and industrial controls for fear of providing information that could be used to exploit their operations. More than 20 of the nation's largest oil companies, including Exxon Mobil Corp. and

ConocoPhillips, refiners Phillips 66 and Valero, service companies Halliburton and Baker Hughes, and pipeline operators Kinder Morgan and Enterprise Products Partners, declined to comment or did not respond to multiple requests for comment. The American Petroleum Institute, the national trade association of oil and gas, declined comment as well.

The Department of Energy has developed a model of best practices while trade groups such as the American Petroleum Institute have adopted industry standards, but none is mandatory.
In recent years, forward-looking oil companies have treated potential cyberattacks on critical assets as a major financial risk, but others haven't taken the threat as seriously, said Charles McConnell, executive director of Rice University's Energy and Environment Initiative.
Oil companies tend to rush to deploy new computer technologies that make operations more productive, he said, but only afterward consider ways to mitigate online threats.
"The pace of change of the technology we've adopted is every step of the way more and more vulnerable to cyberattack," said McConnell, who spent 35 years in the energy industry and served for two years as assistant secretary of energy.

Of nearly 400 U.S. oil employees who specialize in industrial cybersecurity, 61 percent said their companies lack adequate cyber defenses to protect the technologies that run oil and gas facilities, according to a recent survey by the research firm and consultancy Ponemon Institute. Almost seven of 10 respondents said their companies experienced a security breach within the last year, and yet, less than half believe their companies have met industry standards and guidelines for cybersecurity. Oil and gas companies generally have gotten better at securing their information and data systems, Edwards said, but it would be "dangerous" to characterize the progress as universal. Some companies have begun to install firewalls, anti-virus and anti-malware programs and require stricter security measures from equipment manufacturers, among other improvements, cyber security consultants said.

In regulatory filings, Exxon Mobil said its cybersecurity programs block 64 million emails, 139 million internet access attempts and 133,000 other potentially malicious actions each month.
"There are definitely some leaders that have done a lot to stand out," said Robert Lee, a former Air Force cyber warfare operations officer and chief executive of security firm Dragos in San Antonio. "But that's not representative of the industry. It's clear a lot of sites haven't done the minimum for security, and there are many more in the middle."

'Boom in the night'

Devices running automated processes within plants - known as operational technology - were designed years or decades ago before the advent of serious online threats. Security experts say even newer models of sensors and automated controls can't automatically block intrusions.
Marc Othersen, former chief information security officer of New York oil producer Hess Corp., says equipment makers must do more to develop adequately secured devices.

> "The technology offered to us has not closed the gap," he said. "We will always be behind."

Last year, Exxon Mobil and Lockheed Martin announced plans to advance automated systems for refineries and chemical facilities with built-in cyber defenses. The initiative, which includes collaboration with 40 other companies, was prompted primarily because devices with protections strong enough to thwart the most skilled hackers aren't widely available, said Joe Weiss, managing director of the international cybersecurity standards body ISA99.

> "Ironically, it's the most important (of the systems) but the least secure," he said. "That's where you go boom in the night."

If hackers, for example, figured out how to exploit devices running along 2.6 million miles of U.S. pipeline, they could tell a monitoring system the flow of oil and gas has stopped along a pipe, prompting automated systems to begin pumping until they cause a pressure blast. When such systems malfunction, it can lead to disasters on the scale of the 2005 Texas City refinery blast, which killed 15 people and injured 180 more. In that tragedy, there was no malicious intent, but devices were incorrectly calibrated and provided erroneous readings, which, investigators concluded, were major factors leading to the blast.

> "There are a lot of people out there who would love to disrupt (a pipeline) for visual effect … terrorists or other people who want to see black smoke or flames," said Philip Quade, who recently retired as chief of the National Security Agency's cyber task force. "The more strategic threat is what nation-states can do to affect the psyche of the American public."

'In a dark room'

The majority of U.S. oil and gas companies don't have the capability to find or track malware or viruses that have already penetrated control systems, according to Homeland Security, including devices such as sensors and industrial computers. This means hackers can gain access to the systems and root around for months or years seeking weaknesses, collecting sensitive data and lying in wait with viruses that can disrupt operations.

> "We're in a dark room," said Damiano Bolzoni, chief executive of Dutch security firm Security Matters. "Nobody is switching on the light."

Cyber criminals have tried to steal money by sending employees fake invoices. Other hackers lured workers to download malicious software designed to lock people out of computers or other devices until they pay a ransom. In many cases, oil and gas companies wait to react to problems,

said Chris Sistrunk, a consultant with Mandiant, which specializes in cybersecurity. For example, he recalled how an oil company's cybersecurity team was alerted to a security breach, in which a 7-year-old computer worm had been discovered in a Windows operating system. Its presence suggested that the company hadn't updated protection software in at least seven years.

> "Security people are putting out fires instead of hunting for evil on the network," Sistrunk said.

The most sophisticated threats come from hackers backed by foreign governments. Cyber-security researchers say both Russia and China have sponsored hacking groups, often recruited from the cyber-underworld, to probe industrial control systems in the United States and Europe. More recently, hackers allegedly from Russia and China have used phishing emails, infected USB drives and other techniques to penetrate computer networks in broad espionage campaigns against U.S. energy companies aimed at siphoning information about industrial control systems, according to the National Security Agency and cybersecurity firms.

> "These attackers are adaptive and intelligent," said Michael Assante, former chief security officer of the North American Electric Reliability Corp., which regulates the security of electric grids. "That's a scary thing to be up against."

For the most part, federal officials said, cyberattacks against energy companies appear aimed at stealing trade secrets to boost foreign industries and economies. But some officials anticipate that hacker groups may try to gain footholds in pipelines, refineries and power plants, should the day come when a rival nation or extranational group has reason to hold assets hostage or launch a disruptive attack.

> "When the day comes and they need leverage in negotiations or a full-blown act of war, it's not hard to imagine how they might use such a capability," said Barak Perelman, chief executive of the Israeli cyber security firm Indegy.

Quade, the former chief of the NSA's cyber task force, said the threat is more than theoretical, pointing to two viruses launched at energy operations: Stuxnet, which damaged thousands of centrifuges at an Iranian nuclear facility in 2010, and Shamoon, which wiped out computer files in Saudi Arabian oil and gas facilities two years later.

> "In the last five years, we've had repeated demonstrations in the willingness of certain nation-states or other actors to actually use this stuff," Quade said.

It's unlikely that Russia or China would sabotage the nation's energy infrastructure because of the probability of retaliation, but these two world powers have honed their abilities to hold key U.S.

assets hostage and use cyber capabilities to thwart U.S. military responses to online assaults on domestic soil, the U.S. Department of Defense said in a report last month.

> "This emerging situation threatens to place the United States in an untenable strategic position," the Defense Department said.

But security professionals say a major cyberattack against the United States remains a distant possibility, at least for now.

> "They're waiting for a rainy day," said Margrete Raaum, who leads the Norwegian computer emergency response team for the energy sector.

Security vs. costs

Despite improvements, some oil and gas companies still don't make it particularly hard for hackers to get into many systems. Consultants have found lapses in security as egregious as writing passwords of critical computer systems on sticky notes pasted to consoles. Other networks had generally weak passwords or the default passwords set by manufacturers. "There's a lot of those," Edwards said. Part of the problem reflects the culture of the oil and gas industry, said Steve Mustard, an industrial cybersecurity expert at the trade group Automation Federation. Upgrading a multitude of devices could cost millions of dollars, and oil companies often find it too expensive and time-consuming to patch software running multibillion-dollar refineries that produce gasoline almost all the time. Even a four-hour security upgrade can stop production for days, said Philip Hurlston, who works with oil companies and the FBI as oil and gas sector chief at security group InfraGard in Houston. Hurlston says an industry mantra still plagues the mindset of some executives: "Run the equipment until it dies."

Security experts said the steps that energy companies can take to defend against hackers aren't necessarily difficult. It's often a matter of limiting unauthorized access, adopting careful procedures for protecting networks and making sure the latest cybersecurity measures are in place. The question remains, however, how quickly companies are moving to take such actions, and perhaps more fundamentally, how seriously do they take the threat.

> "For an oil executive, worrying about a cyberattack sounds like science fiction," said Brett Young, a consultant and founder of the cyber security collaborative, OpenICS Project. "It's like worrying about a meteor strike."

S 133 Introduced – FY 2017 Intelligence Authorization, 2017, by Patrick Coyle (news blog)

Earlier this month Sen. Burr (R, NC) introduced S 133, the Intelligence Authorization Act for Fiscal Year 2017. Last Friday the Senate Select Committee on Intelligence reported the bill

favorably without amendment. There are two cybersecurity provisions that may be of interest to readers of this blog:

Sec. 312. Assistance for nationally significant critical infrastructure.
Sec. 614. Report on cybersecurity threats to seaports of the United States and maritime shipping.

CI Assistance

Section 312 would authorize elements of the intelligence community, through the Under Secretary for Intelligence and Analysis of the Department of Homeland Security, to provide assistance to covered critical infrastructure facilities "to reduce the risk of regional or national catastrophic harm caused by a cyber-attack (sic) against covered critical infrastructure" {§312(c)}.

A key term used in §312 is 'covered cybersecurity asset' which is defined as "an information system ***or industrial control system*** [emphasis added] that is essential to the operation of covered critical infrastructure" {§312(a)(2)}.

The bill describes the type of assistance to be provided by the intelligence community. It includes {§312(e)(2)}:

- Activities to develop a national strategy to effectively leverage intelligence community resources made available to support the program;
- Activities to consult with the Director of National Intelligence and other appropriate intelligence and law enforcement agencies to identify within the existing framework governing intelligence prioritization, intelligence gaps and foreign intelligence collection requirements relevant to the security of covered cyber assets and covered critical infrastructure;
- Activities to improve the detection, prevention, and mitigation of espionage conducted by foreign actors against or concerning covered critical infrastructure;
- Activities to identify or provide assistance related to the research, design, and development of protective and mitigation measures for covered cyber assets and the components of covered cyber assets; and
- Activities to provide technical assistance and input for testing and exercises related to covered cyber assets.

Cybersecurity Threats to Seaports

Section 614 would require the Under Secretary of Homeland Security for Intelligence and Analysis to submit a report to Congress on cybersecurity threats to seaports and maritime shipping. The report would address "the cybersecurity threats to, and the cyber vulnerabilities within, the software, communications networks, computer networks, or other systems" {§614(a)}. While it does not specifically address control systems, the 'other systems' mention probably provides for coverage of that topic.

In addition to a report on any recent cyber-attacks or cybersecurity threats, the bill would require an assessment of {§614(b)}:

• Any planned cyber-attacks directed against such software, networks, and systems;
• Any significant vulnerabilities to such software, networks, and systems; and
• How such entities and concerns are mitigating such vulnerabilities.

While not specifically stated, the report will almost certainly be classified because of the requirement to be "consistent with the protection of sources and methods" {§614(a)}.

Moving Forward

This bill was supposed to have been a 'must pass' bill in the last session. The House passed three slightly different versions of an intel authorization bill and the Senate Select Committee on Intelligence marked up their own version of such a bill, but nothing made its way to the Senate floor. With most of the players remaining the same in the Senate, it will be interesting to see if the change in administration has any potential effect on the consideration of this bill.

Common Sense Operational Security, March 24, 2017, Paul Martin (USCG)

For those of us who work in one of our nation's military services, Operatinal Security (OPSEC) is an everyday concern. We receive annual training on the subject and practice it daily. This applies to cybersecurity as well, specifically the handeling of e-mails, phone texts, and social media. While the following guidance comes from the **Defence Department's Office of OPSEC**, many of these **Best Practices and Recommendations** (DES OPSEC, 2017, Michael Chesbro) could apply to any business.

E-mail: Encryption should be used when sending e-mail that contains any type of non-public information. Even public information can reveal an organization's focus, interest, and concerns. Regularly published official journals, bulletins, briefs, and information updates, if sent by e-mail, must be encrypted.

> *Many word processing programs allow you to encrypt a document, which, can then be placed into an e-mail as an attachment. Send the password for the encrypted document as a separate e-mail using a different subject line.*

Do NOT auto-forward e-mail: auto-forward can result in unauthorized disclosure of sensitive information, and can result in data spillage or the spread of malware.

Do NOT use e-mail as a file storage system: delete e-mail once it has been read and responded to. If information in an e-mail must be retained, save it as a separate file or document.

BCC: when sending e-mail to large numbers of recipients, use Blind Carbon Copy (BCC). Keep in mind that many people do not want their e-mail address and other personal information disclosed to someone that they do not know. BCC helps to reduce Spam since BCC addresses cannot be seen and harvested by Spammers and BCC messages cannot not be used, by an adversary, to develop lists of names of the employees of a company or members of an organization since, again, the names and email addresses of the recipients are not visible. It should also be noted that NIST Special Publication 800122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" lists e-mail addresses as one type of PII. As a government employee, you have specific legal requirements to safeguard PII.

Out-of-Office Messages: Limit the amount of information you put in out-of-office messages. Use a generic message such as: "I am currently out of the office. If you need immediate assistance, please call (123) 456-7890. Otherwise, I will reply upon my return." Do not include the date of your return or the name of whomever will answer the listed phone number while you are gone.

Text Messages: Never send sensitive information or other work-related, nonpublic, information via text message. Text messages, as a rule, can be read and stored by your phone company or by surveillance and monitoring equipment in the area. According to the American Bar Association:

> "While text messages have increasingly replaced phone calls, users do not always stop and realize that individually identifiable information, once captured in a traditional text message or thirdparty messaging system, likely becomes a PII record."

Consumer text messaging services also offer little protection from sending messages to an unintended recipient. Texting a personal message to the wrong recipient can be embarrassing, but text messaging PII to the wrong person potentially carries significant consequences. Indeed, a single text message including PII sent to the wrong number or wrong person would likely constitute a PII breach and (U.S. Government's) Privacy Act Violation.

Social Media: Keep your professional life and your personal life separate on social media. Never use social media as a crime or suspicious activity reporting tool. Review the DOD Identity Awareness, Protection, and Management Guide for tips of how to secure your social media accounts.

Need to Know: Only distribute information to people who have an official need to know the information in the performance of their duties. If you are receiving distribution from other agencies make sure that you actually need that information for the performance of your duties. Comply with the 'third party rule' which restricts the dissemination of non-public information outside of your agency.

According to press reports about the "Sony Hack Scandle" of a few years ago; the hackers gained some of the information they needed to hack Sony by trolling the social media accounts of various Sony officials. Once hacked, scandalous e-mail descriptions about promonent persons were exposed causing the company harm; it is likely that important business information was likewise compromised. *Bottom Line – safeguarding information both professional and personal is an everyday chore that we should all be mindful of.*

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report cyber intrusions and every other security breach to the Coast Guard's National Response Center (NRC):

- Phone 1-800-424-8802 or direct phone line at 202-372-2428
- Fax 202-372-2920
- Web: http://www.nrc.uscg.mil/

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- IngraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.