NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
October 2014 (edition 2014-1)

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 contain 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

- **Reporting Cyber Security Threats** – current Coast Guard stance on reporting cyber security incidents and threats.
- **Global Shipping Fleet Exposed to Hacking** – discusses "at sea" cyber intrusions and attacks; and vulnerabilities of various important data systems to intrusion. Industry dependence on computerized systems makes vessels, facilities and platforms more vulnerable. Software from manufacturers may have known "flaws" that make them more susceptible to intrusion.
- **Cargo Theft Investigation** – authorities found GPS "jammers" being used as part of a cargo theft operation.
- **Computer Hacking can Hide Spyware Instillation** – apparent "less destructive" cyber attacks can be used to mask the instillation of spyware on a computer system.

- **U.S. Army Hacked** – members of an international operation were caught hacking and stealing software used by the U.S. Army to train personnel.**FBI Releases Malware Investigator Portal to Industry** – The FBI's Malware Investigator portal will soon be available to security researchers, academics and businesses. The Malware Investigator analyses threats through sandboxing, file modification, section hashing, correlation against other submissions and the FBI's own entries concerning viruses and malware reports.
- **California OES – Social Media Exploited** – discusses common social media scams and common sense steps to protect yourself.
- **SASC Investigation Finds Chinese Intrusions** – Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military's system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found.
- **National Cybersecurity Institute (NCI) Courses** – National Cybersecurity Institute (NCI) is an academic and research center located in Washington D.C. dedicated to assisting government, industry, military and academic sectors meet the challenges in cyber security policy, technology and education. NCI has online (distance learning) courses for certificates available.

MAIN ARTICLES

United States Coast Guard (3/5/14)

Cyber intrusions are to be treated just like other suspicious activity reports to/through the NRC:

- The Coast Guard's current posture is one of education, not enforcement.
- Cyber incidents and related threats (for informational purposes to partners) should be disseminated (when appropriate/able) via Homeport.
- MTSA regulated facilities should report cyber incidents to the NRC, much like any other security incident.

"While Coast Guard cyber security requirements for the Maritime Transportation System (MTS) are still in development, the Coast Guard is requesting information concerning exploitation and misuse of the cyber environment, with an emphasis on activities that threaten the order and function of the MTS, to improve the Coast Guard's ability to carry out the Coast Guard's Maritime Security mission. To summarize, the new Coast Guard Standing Requirement (CGSR) 001-14 requests the reporting of unusual or suspicious cyber activity affecting MTS infrastructure; MTS owners and operators' discovery of physical surveillance or attempt to access the operational control systems used to manage MTS equipment; confirmed or suspected MTS infrastructure cyber-attacks; and unusual use or possession of hardware, software, or equipment (to include WI-FI antennas and other communication equipment) to gain access to port facilities. It is important that MTS owners/operators understand that the requirements in the

CGSR are not indicative of future intentions concerning MTS based cyber security requirements and instead fulfill a Coast Guard need for information to carry out its Maritime Security Mission. Please coordinate all reporting efforts related to this CGSR with Sector Prevention staffs."

Federal Bureau of Investigation (5/15/14) – All at Sea: Global Shipping Fleet Exposed to Hacking Threat, Wed, Apr 23 2014, By Jeremy Wagstaff

SINGAPORE (Reuters) - The next hacker playground: the open seas - and the oil tankers and container vessels that ship 90 percent of the goods moved around the planet. In this internet age, as more devices are hooked up online, so they become more vulnerable to attack. As industries like maritime and energy connect ships, containers and rigs to computer networks, they expose weaknesses that hackers can exploit. Hackers recently shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again; Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they're somewhere else; and hackers infiltrated computers connected to the Belgian port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records.

While data on the extent of the maritime industry's exposure to cyber crime is hard to come by, a study of the related energy sector by insurance brokers Willis this month found that the industry "may be sitting on an uninsured time bomb". Globally, it estimated that cyber attacks against oil and gas infrastructure will cost energy companies close to $1.9 billion by 2018. The British government reckons cyber attacks already cost UK oil and gas companies around 400 million pounds ($672 million) a year. In the maritime industry, the number of known cases is low as attacks often remain invisible to the company, or businesses don't want to report them for fear of alarming investors, regulators or insurers, security experts say.

There are few reports that hackers have compromised maritime cyber security. But researchers say they have discovered significant holes in the three key technologies sailors use to navigate: GPS, marine Automatic Identification System (AIS), and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS). "Increasingly, the maritime domain and energy sector has turned to technology to improve production, cost and reduce delivery schedules," a NATO-accredited think-tank wrote in a recent report. "These technological changes have opened the door to emerging threats and vulnerabilities as equipment have become accessible to outside entities."

Tip Of The Iceberg

As crews get smaller and ships get bigger, they increasingly rely on automation and remote monitoring, meaning key components, including navigational systems, can be hacked. A recent study by security company Rapid7 found more than 100,000 devices - from traffic signal equipment to oil and gas monitors - were connected to the internet using serial ports with poor security. "The lines get blurry, and all industries and all technologies need to focus more on security," said Mark Schloesser, one of the authors of the study. Mark Gazit, CEO of ThetaRay, an internet security company, said an attacker managed to tilt a floating oil rig to one side off the coast of Africa, forcing it to shut down. It took a week to identify the cause and fix, he said, mainly because there were no cyber security professionals aboard. He declined to say more. Lars Jensen, founder of CyberKeel, a maritime cyber security firm, said ships often switch off their AIS systems when passing through waters where Somali pirates are known to operate, or fake the data to make it seem they're somewhere else. Shipping companies contacted by Reuters generally played down the potential threat from hackers. "Our only concern at this stage is the possible access to this information by pirates, and we have established appropriate countermeasures to handle this threat," said Ong Choo Kiat, president of U-Ming Marine Transport, Taiwan's second-largest listed shipping firm by market value. The company owns and operates 53 dry cargo ships and oil tankers.

Virus-Riddled

A study last year by the Brookings Institution of six U.S. ports found that only one had conducted an assessment of how vulnerable it was to a cyber attack, and none had developed any plan to response to any such attack. Of some $2.6 billion allocated to a federal program to beef up port security, less than 1 percent had been awarded for cyber security projects. When CyberKeel probed the online defenses of the world's 20 largest container carriers this year it found 16 had serious security gaps. "When you look at the maritime industry there's extremely limited evidence of systems having been breached" compared to other sectors, said CyberKeel's Jensen. "That suggests to us that they've not yet been found out." Michael Van Gemert, a security consultant to the oil and gas industry, said that on visits to rigs and ships he has found computers and control systems riddled with viruses. In one case, he said it took 19 days to rid a drilling rig en route from South Korea to Brazil of malware which had brought the vessel's systems to a standstill. "The industry is massively in need of help, they have no idea what the risks are," he said. The main ship navigation systems - GPS, AIS and ECDIS - are standards supported by bodies such as the International Maritime Organization (IMO). Indeed, that body has made AIS and ECDIS mandatory on larger commercial and passenger vessels.

Researchers from the University of Texas demonstrated last July that it was possible to change a ship's direction by faking a GPS signal to dupe its onboard navigation system. Marco Balduzzi

and colleagues at anti-virus vendor Trend Micro last month showed that an attacker with a $100 VHF radio could exploit weaknesses in AIS - which transmits data such as a vessel's identity, type, position, heading and speed to shore stations and other ships - and tamper with the data, impersonate a port authority's communications with a ship or effectively shut down communications between ships and with ports. In January, a British cyber security research firm, NCC Group, found flaws in one vendor's ECDIS software that would allow an attacker to access and modify files, including charts. "If exploited in a real scenario," the company concluded, "these vulnerabilities could cause serious environmental and financial damage, and even loss of life."

When the USS Guardian ran aground off the Philippines last year, the U.S. Navy in part blamed incorrect digital charts. A NATO-accredited think-tank said the case illustrated "the dangers of exclusive reliance upon electronic systems, particularly if they are found vulnerable to cyber attack." "Most of these technologies were developed when bandwidth was very expensive or the internet didn't exist," said Vincent Berk, CEO of security company FlowTraq.

No Quick Fix

Fixing this will take time, and a change in attitude. "Security and attack scenarios against these technologies and protocols have been ignored for quite some time in the maritime industry," said Rapid7's Schloesser. Researchers like Fotios Katsilieris have offered ways to measure whether AIS data is being faked, though he declined to be interviewed, saying it remained a sensitive area. One Google researcher who has proposed changes to the AIS protocol wrote on his blog that he had been discouraged by the U.S. Coastguard from talking publicly about its vulnerabilities. Indeed, AIS is abused within the industry itself. Windward, an Israeli firm that collects and analyses AIS data, found 100 ships transmitting incorrect locations via AIS in one day - often for security or financial reasons, such as fishing boats operating outside assigned waters, or smuggling.

In a U.N. report issued earlier this year on alleged efforts by North Korea to procure nuclear weapons, investigators wrote that one ship carrying concealed cargo turned off its AIS signals to disguise and conceal its trip to Cuba. It's not clear how seriously the standards bodies treat the threat. Trend Micro's Balduzzi said he and his colleagues were working with standards organizations, which he said would meet next year to discuss his research into AIS vulnerabilities. The core standard is maintained by the International Telecommunications Union (ITU) in association with the IMO. In a statement, the IMO said no such report of vulnerabilities had been brought to its attention. The ITU said no official body had contacted it about the vulnerabilities of AIS. It said it was studying the possibility of reallocating spectrum to reduce saturation of AIS applications. Yevgen Dyryavyy, author of the NCC report on ECDIS, was skeptical that such bodies would solve the problems soon. First, he said, they have to understand

the IT security of shipboard networks, onboard linked equipment and software, and then push out new guidelines and certification. Until then, he said, "nothing will be done about it." ($1 = 0.5949 British Pounds)

Federal Bureau of Investigation (7/14/14) – Cargo Theft in the Port of Miami

There was a cargo theft of a temperature controlled shipment housed in refer trailer, in North Florida. In that theft scenario the hauling tractors were swapped out – a common methodology for south Florida cargo thieves. The Miami based suspects involved were ultimately stopped and apprehended by the Florida Highway Patrol in mid-Florida - on a routine vehicle stop. The shipment was recovered intact. Discovered, hidden inside of the trailer's refer unit, was a portable GPS jamming device - hooked to a battery inside the refer for power. What's unique about the trailer is that it was not equipped with a visible GPS tracking device – in point of fact, there was no GPS device on or in the trailer at all. It is reasonable to conclude, then, that the individuals who planted the jammer felt that there may have been a tracking device secreted somewhere inside the shipment. This reported is one of the first, confirmed, uses of a GPS jamming device here in the United States.

Federal Bureau of Investigation (7/17/14) – Ports urged to beware no theft hacks IHS Maritime's Jon Guy reveals that what seem to be simple computer break-ins can mask installation of spyware and viruses:

Criminals are using 'cyber-feint' tactics – diversionary IT system break-ins – as they step up attacks on computer and technology systems of ports and logistics companies. Both illegal and high-value legitimate cargoes are targets, Mike Yarwood, claims chief for the international transport, freight and logistics insurance provider TT Club, has warned. Ports and terminals are increasingly detecting seemingly failed electronic break-ins in which nothing turns out to be stolen, he told IHS Maritime. In fact, these are used to mask attempts by criminals to place spyware and viruses in computer systems to facilitate more serious crimes, he explained.
His warning comes as insurers are increasingly concerned that cyber-attacks are fast becoming the new piracy, targeting systems that are outdated and open to hacking. As invasive cyber-technology becomes more widely available, a greater risk to legitimate trade is emerging, exposing operators in the supply chain to economic and commercial damage, Yarwood cautioned. Advances in IT systems undoubtedly provide greater opportunities for carriers, transport operators, and cargo handling facilities to mitigate their exposure to theft and fraud, he noted, but such increased sophistication also benefits those with criminal intent. The TT Club is well placed to observe and analyse both the nature and effect of such cyber-crime, according to Yarwood, whose claims desk is studying the emerging threat. Shipping companies need to take immediate action, he declared.

"We see incidents that at first appear to be a petty break-in at office facilities. The damage appears minimal. Nothing is physically removed. More thorough investigations, however, reveal that the thieves were actually installing spyware within the operator's IT network." The study

found that the most common targets were individuals' personal devices, where cyber security is less adequate than it is for office systems. Hackers often use social networks to target operational personnel who travel extensively and truck drivers to ascertain routeing and overnight parking patterns, he cautioned. The TT Club said the type of information being sought and extracted might be release codes for containers from terminal facilities or passwords to discover delivery instructions. The intent is to facilitate import and export of illegal substances and traffic of human cargoes; others target containers with high-value legitimate content.

Yarwood referred to "an apparent focus on specific individual containers in attempts to track the units through the supply chain to the destination port. Such systematic tracking is coupled with compromising the terminal's IT systems to gain access to, or generate release codes for, specific containers. "Criminals are known to have targeted containers with illegal drugs in this way. However, such methods also have greater scope in facilitating high-value cargo thefts and human trafficking." In high-profile cases, computer systems have been attacked at major European ports to allow criminals to remove boxes transporting high-value content, Yarwood noted, adding that the TT Club was advising clients to be increasingly vigilant. "Often the level of threat is dependent on an organisation's own culture," he said. **This article appeared in IHS Maritime Fairplay magazine, 10 July 2014.**

Hackers Exploit U.S. Army, Microsoft (Govinfosecurity, 10/1/14)

Four alleged members of an international hacking ring have been charged by U.S. authorities with using malware and SQL injection attacks to steal intellectual property valued at more than $100 million from the U.S. Army, Microsoft, as well as game-makers Epic, Valve and Zombie.

"The members of this international hacking ring stole trade secret data used in high-tech American products, ranging from software that trains U.S. soldiers to fly Apache helicopters to Xbox games," says Leslie Caldwell, the Assistant Attorney General of the Justice Department's criminal division. According to the U.S. indictment, the gang allegedly regularly employed malware and SQL injection attacks to steal credentials that allowed them to access targeted websites. All told, the gang allegedly stole tens of thousands of usernames, and committed numerous counts of identity theft, in part by using people's stolen personal information to submit applications for credit card accounts with limits of up to $20,000.

FBI releases Malware Investigator portal to industry players (ZD Net, 9/30/14)

The FBI's Malware Investigator portal will soon be available to security researchers, academics and businesses. As reported by Threatpost, the US law enforcement agency's tool is akin to systems used by cybersecurity companies to upload suspicious files. Once a file is uploaded, the system pushes through antimalware engines to pull out information on the file -- whether it is malicious, what the malware does, and whom it effects. The Malware Investigator analyses threats through sandboxing, file modification, section hashing, correlation against other submissions and the FBI's own entries concerning viruses and malware reports. Windows files

and common file types can currently be analyzed, but this will expand to include other file types in the near future.

Employee Security Awareness Is Key to Reducing Deficiencies

Protecting classified information depends more than ever on the human element of security -- employees. The sad fact is, employees are still the weakest link in the security chain because they're not trained to be security-conscious. Industry studies reveal that lax employee attitudes and mistakes are the #1 cause of security breaches and "deficiencies". And when government reps visit your facility during regular and unannounced inspections, it's not the security department they'll be focusing on -- it's your employees!

CEO indicted for company's alleged mobile spyware app (ComputerWorld, 9/29/14)

The CEO of a Pakistani company has been indicted in the U.S. for selling a product called StealthGenie that buyers could use to monitor calls, texts, videos and other communications on other people's mobile phones, the U.S. Department of Justice said. The indictment of Hammad Akbar, 31, of Lahore, Pakistan, represents the first time the DOJ has brought a criminal case related to the marketing and sale of an alleged mobile spyware app, the DOJ said in a press release Monday. Akbar is CEO of InvoCode, the company selling StealthGenie online. Akbar is among the creators of StealthGenie, which could intercept communications to and from mobile phones, including Apple, Android and BlackBerry devices, the DOJ said. StealthGenie was undetectable by most people whose phones it was installed on and was advertised as being untraceable, the DOJ said.

Hackers Exploit Shellshock, Much More Trouble Awaits (CIO Today, 9/28/14)

Security experts are keeping an eye on the Shellshock vulnerability, also known as the Bash (Bourne-Again Shell) bug, as a focus for malicious scanning and at least one botnet. They warn, though, that hackers haven't even begun to test the limits of the vulnerability. The Shellshock vulnerability, also called the Bash (Bourne-Again Shell) bug, could be even an even greater threat than the Heartbleed bug. Disclosed in April, Heartbleed threw a scare into Internet users by exploiting OpenSSL cryptography vulnerabilities to allow theft of servers private keys and users' session cookies and passwords via fake Web sites. The Internet security firm FireEye reported that it has seen plenty of malicious traffic using the Bash bug, some of it possibly from Russia. The activity has included DDoS attacks, malware droppers, reverse shell hacks, backdoors and data exfiltration.

California Office of Emergency Services (9/30/14) – Social Media Exploited

The use of social media has exploded, with 255 million active users on Twitter and more than 1.2 billon on Facebook. Unfortunately, so too have the scams and attacks that target social media. Criminals are taking advantage of the increasing number of users and the enormous amount of information exchanged.

What are Some Common Scams?

1. Information about special events (such as the Olympics), or tragedies (such as the missing Malaysian Airliner) could be used by those with malicious intent to conduct social engineering scam, particularly on social media. For example, many individuals are tempted to click on a video they see on their "newsfeed." Unfortunately, these videos may lead to a malicious website designed to infect your computer.

2. Typical scams feature notices of items that can be "free" for you or available at a very low price. If you notice an online advertisement about the newest tech gadget, at a ridiculously low cost, it is most likely a scam to trap users into clicking on the ad. Sometimes a refundable deposit is requested, other times, direct access to your Facebook account requested. These are scams intending to victimize you and your friends.

Fake organizations claiming to be charities have mushroomed on social media sites. They often post heart-wrenching images, such as a picture of babies with serious diseases or a fire that destroyed an entire community – basically anything that will appeal to people's emotions. These posts almost always include a call-to-action, such as pleas for donations. Avoid being a victim. Investigate the legitimacy of these organizations before contributing.

What Precautions can be taken?

- Do not post private and confidential information, such as your credit card number, password or other personal information.
- Install anti-virus software, proper firewalls, and anti-malware programs on your devices, including desktops, laptop, smartphones, tables, etc., that you use to access social networking sites.
- Inspect a link before clicking on it. If it seems suspicious, trust your instincts and don't click, even if the link has supposedly originated from someone you know and trust. It is possible that their account was compromised, and could be spreading malware without their knowledge.
- When posting images, change settings accordingly to ensure they are private and can be viewed only by people whom you trust. If you delete your account, make sure all data and pictures are removed.
- Third party applications provided by social networking sites might not have the same privacy policy or security model as the social media site. You should not allow these apps to have complete access to your account; your personal data can be stolen or misused.
- Use strong, unique passwords that only you know. Each account on social media should have varied passwords.

Federal Bureau of Investigation (9/19/14) – SASC investigation finds Chinese intrusions into key defense contractors report describes threats to transportation systems, gaps in reporting requirements. Wednesday, September 17, 2014

WASHINGTON – Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year,

intrusions that show vulnerabilities in the military's system to deploy troops and equipment in a crisis, a Senate Armed Services Committee investigation has found. The year-long investigation found that TRANSCOM, which is responsible for global movement of U.S. troops and equipment, was only aware of two of those intrusions. It also found gaps in reporting requirements and a lack of information sharing among government entities that left the command largely unaware of computer compromises by China of contractors that are key to the mobilization and deployment of military forces. These and other findings are included in a report, "Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors," that the committee approved unanimously this spring. The committee released an unclassified version of the report today.

"These peacetime intrusions into the networks of key defense contractors are more evidence of China's aggressive actions in cyberspace," said Sen. Carl Levin, D-Mich., the committee's chairman. "Our findings are a warning that we must do much more to protect strategically significant systems from attack and to share information about intrusions when they do occur." "We must ensure that cyber intrusions cannot disrupt our mission readiness" said Senator Jim Inhofe, R-OK, the committee's ranking member. "It is essential that we put into place a central clearinghouse that makes it easy for critical contractors, particular those that are small businesses, to report suspicious cyber activity without adding a burden to their mission support operations."

The committee investigation focused on a little-recognized but vital U.S. military asset: the ability to tap civilian air, shipping and other transportation assets to rapidly deploy U.S. forces in times of crisis. Through programs such as the Civil Reserve Air Fleet, commercial transportation companies, some of whom do little or no CRAF-related business in peacetime, become key elements of TRANSCOM's plans for moving troops and equipment around the world.
The committee found that in a 12-month period beginning June 1, 2012, there were about 50 intrusions or other cyber events into the computer networks of TRANSCOM contractors. At least 20 of those were successful intrusions attributed to an "advanced persistent threat," a term used to designate sophisticated threats commonly associated with governments. All of those intrusions were attributed to China. Among the investigation's findings:

- A Chinese military intrusion into a TRANSCOM contractor between 2008 and 2010 that compromised emails, documents, user passwords and computer code.
- A 2010 intrusion by the Chinese military into the network of a CRAF contractor in which documents, flight details, credentials and passwords for encrypted email were stolen.
- A 2012 Chinese military intrusion into multiple systems onboard a commercial ship contracted by TRANSCOM.

The investigation found significant gaps in information sharing regarding cyber intrusions. A committee survey of a small subset of TRANSCOM contractors discovered 11 intrusions by China into contractor networks. The investigation also found that the FBI or DoD were aware of at least nine other successful intrusions by China into TRANSCOM contractors. Of those 20 intrusions, TRANSCOM was only made aware of two.
That gap was in part a result of contractors and TRANSCOM lacking a common understanding of what intrusions ought to be reported to TRANSCOM. Also, DoD agencies lack a clear

understanding as to what information about cyber intrusions can and should be shared with TRANSCOM and other agencies within the Department.

The committee also found that cyber intrusion reporting requirements are focused on intrusions that affect DoD data. Some TRANSCOM contractors, such as several CRAF airlines, however, may do little or no business with the military until called upon in a crisis. Peacetime intrusions at those companies may not involve immediate loss of military information, but could leave those companies vulnerable to loss of information or disruption of operations when they are activated to support military operations.

In response to the investigation's findings, the committee included a provision in its version of the National Defense Authorization Act for Fiscal Year 2015 directed at addressing reporting gaps and improving the way in which the Department disseminates information about cyber intrusions into the computer networks of operationally critical contractors. Specifically, the provision directs the Secretary of Defense to establish procedures for designating companies as ''operationally critical contractors'' and tightening requirements that those contractors report successful cyber penetrations by known or suspected government actors. It also requires DoD to establish new procedures to assist contractors in detecting and mitigating cyber threats while ensuring protections for trade secrets, commercial or financial information. The provision requires the Secretary to assess existing reporting requirements and DoD policies and systems for sharing information on cyber intrusions. It also requires the Secretary to designate a single DoD component to receive intrusion reports from contractors and other government agencies and to issue guidance ensuring that intrusion-related information is shared with appropriate DoD components.

Federal Bureau of Investigation (10/2/14) – National Cybersecurity Institute (NCI) Courses.

The National Cybersecurity Institute (NCI) is an academic and research center located in Washington D.C. dedicated to assisting government, industry, military, and academic sectors meet the challenges in cyber security policy, technology and education. Most importantly, they offer distance learning on cybersecurity including http://www.nationalcybersecurityinstitute.org/ Excelsior College offers six academic programs at the undergraduate and graduate levels in cybersecurity:

- Undergraduate Cybersecurity Certificate <http://www.excelsior.edu/programs/technology/cybersecurity-undergraduate-certificate>
- Bachelor of Science in Cyber Operations <http://www.excelsior.edu/programs/technology/cyber-operations-bachelor-degree>
- Bachelor of Science in Information Technology in Cybersecurity Technology <http://www.excelsior.edu/programs/technology/information-technology-cybersecurity-technology-bachelor-degree>
- Master of Business Administration with Cybersecurity Management Concentration <http://www.excelsior.edu/programs/business/mba-cybersecurity-management-master-degree>

- Master of Science in Cybersecurity <http://www.excelsior.edu/programs/technology/cybersecurity-master-degree>
- Graduate Cybersecurity Management Certificate <http://www.excelsior.edu/programs/technology/cybersecurity-management-graduate-certificate>

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) also wants to 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.