U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7501
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7501
Staff Symbol: CG-5P
Phone: (202) 372-1111
Fax: (202) 258-2258

16000
CG-5P Policy Letter
No. 08-16

Digitally signed by CALHOUN.SCOTT.R.1118195147
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USCG, cn=CALHOUN.SCOTT.R.1118195147
Date: 2016.12.16 11:36:23 -05'00'

14 December 2016

From: P. F. Thomas, RADM
COMDT (CG-5P)

To: Distribution

Subj: REPORTING SUSPICIOUS ACTIVITY AND BREACHES OF SECURITY

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) 46 United States Code (USC) part 70103 (c) (3) (A)
(c) Information Sharing Environment (ISE) for Suspicious Activity Reporting (ISE-FS-200)
(d) National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms, NISTIR 7298 Revision 2
(e) NIST Cybersecurity Framework, version 1.0

1. Purpose. Promulgate policy for use by Maritime Transportation Security Act (MTSA) regulated vessels and facilities outlining the criteria and process for suspicious activity (SA) and breach of security (BoS) reporting.

2. Action. Coast Guard Captains of the Port (COTP), Area Maritime Security Committees (AMSC), and the operators of vessels and facilities regulated by the MTSA may use this policy letter when evaluating SA and BoS reports. This policy letter will be distributed by electronic means only. It is available by accessing the MTSA page on Homeport.

   A. The U.S. Coast Guard appreciates the vigilance, professionalism, and patriotism of the marine industry in maintaining security standards. Maritime security is a shared responsibility, and reports of SA and BoS are an important part of our efforts to protect the Marine Transportation System (MTS) from attack.

   B. An owner or operator of a vessel or facility that is required to maintain an approved security plan in accordance with parts 104, 105 or 106 of Reference (a) shall, without delay, report activities that may result in a Transportation Security Incident (TSI) to the National Response Center (NRC), including SA or a BoS. The primary purpose of this requirement is to allow the COTP opportunity to understand and respond to potential threats to the port area upon receipt of a report from the NRC, and to assess the adequacy of security plans to prevent a TSI. Additionally, IAW Reference (b), the Facility Security Plan (FSP) shall "be consistent with the requirements of the National Transportation

Security Plan and Area Maritime Transportation Security Plans." The COTP will affirm consistency to help ensure alignment of SA and BoS communication procedures within FSPs throughout their area of responsibility.

C. The maritime industry continues to expand its use of networked technology, which creates efficiencies but also increases threats and vulnerabilities to vessels and facilities through telecommunications equipment, computers, and networks. Due to the increasing reliance on telecommunications equipment, computers, and networked systems for controlling physical operations, a growing portion of all security risks have a network or computer nexus. Maintaining the security of these systems, including reporting network or computer related SA or BoS, is vital to maintaining the security of the MTS.

D. Plausible terrorist attack scenarios include combined cyber and physical incidents. Vessel and facility operators should consider this possibility when evaluating a cyber incident, including the possibility that a cyber incident is a precursor to a physical attack, or that cyber related SA and BoS may be an attempt by actors to identify weaknesses or to plan for later attacks.

E. The target and intent of malicious cyber activity can be difficult to discern. The fact that business and administrative systems may be connected to operational, industrial control and security systems further complicates this matter. The Coast Guard strongly encourages vessel and facility operators to minimize, monitor, and wherever possible, eliminate any such connections.

F. The U.S. Coast Guard handles all reports of security incidents as Sensitive Security Information (SSI), in accordance with 49 CFR part 1520, which includes requirements for proper marking and storage. The information is therefore not subject to routine public disclosure. The U.S. Coast Guard will share the information with other law enforcement agencies on a need to know basis.

3. Policy. The following criteria describe U.S. Coast Guard requirements for reporting BoS and SA for both physical and network or computer-related events. No description could cover all possible events and vessel and facility operators shall use their best judgment in making reports.

A. Breach of Security

i. U.S. Coast Guard regulations define a breach of security as "an incident that has not resulted in a TSI but in which security measures have been circumvented, eluded, or violated." This definition includes the breach of telecommunications equipment, computer, and networked system security measures where those systems conduct or support functions described in vessel or facility security plans or where successful defeat or exploitation of the systems could result or contribute to a TSI.

ii. BoS incidents may include, but are not limited to, any of the following:

a) Unauthorized access to regulated areas;

b) Unauthorized circumvention of security measures;

c) Acts of piracy and/or armed robbery against ships;

d) Intrusion into telecommunications equipment, computer, and networked systems linked to security plan functions (e.g., access control, cargo control, monitoring), unauthorized root or administrator access to security and industrial control systems, successful phishing attempts or malicious insider activity that could allow outside entities access to internal IT systems that are linked to the MTS;

e) Instances of viruses, Trojan Horses, worms, zombies or other malicious software that have a widespread impact or adversely affect one or more on-site mission critical servers that are linked to security plan functions; and/or

f) Any denial of service attacks that adversely affect or degrade access to critical services that are linked to security plan functions.

iii. Note that routine spam, phishing attempts, and other nuisance events that do not breach a system's defenses are NOT BoS. Furthermore, breaches of telecommunications equipment, computer, and networked systems that clearly target business or administrative systems unrelated to safe and secure maritime operations are outside the U.S. Coast Guard's jurisdiction and need not be reported to the U.S. Coast Guard.

B. Suspicious Activity

i. Reference (c) defines SA as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."

ii. Computer-related suspicious activity presents additional vulnerabilities, and companies should be able to distinguish untargeted cyber incidents from targeted incidents on vessel or waterfront facility computer related systems. Untargeted cyber incidents are part of the normal information technology landscape and commonly include "phishing" or persistent scanning of networks, and these are not considered SA or BoS.

iii. In contrast, targeted incidents may be large, sustained attacks on important cyber systems in an apparent attempt to exploit them for nefarious purposes. Spear phishing campaigns, a marked increase in network scanning, or other attacks may be considered SA if the volume, persistence, or sophistication of the attacks is out of the ordinary.

iv. Unsuccessful but apparently targeted incidents may be SA if they threaten systems that could contribute to a TSI, have a link to the MTS portion of the facility or are otherwise related to systems, personnel, and procedures addressed by security plans or MTSA requirements.

v. SA may include, but is not limited to, any of the following:

a) Unfamiliar persons in areas that are restricted to regular employees;

b) Unusual behavioral patterns, such as:

(1) Not responding to verbal interaction;

(2) Walking slowly in a deliberate fashion towards a potential target;

(3) Inappropriately dressed (e.g., wearing excessive clothing as to conceal something, or looking out of place);

(4) Excessive nervousness or “doomsday” talk;

(5) Excessive questions;

(6) Lack of photo identification;

(7) Agitation or rage;

(8) Picture taking, especially if the suspect has been asked earlier not to take photos;

(9) Note taking or drawing;

(10) Taking measurements; and/or

(11) Attempting to access unauthorized areas.

c) Potentially dangerous devices found by screeners prior to loading persons or cargo or items found on or near the facility that seem out of place.

d) Vehicles parked or standing for excessive amounts of time near the facility perimeter;

e) Unmanned Aircraft System (UAS) activity, including but not limited to:

(1) Reconnaissance and surveillance activities, indicated by repeated activities at a particular place and time (e.g., fly-overs, hovering at low altitudes, and prolonged time on station); and/or

(2) Testing of facility security protocols using UAS, indicated by flying by a target, moving into sensitive areas, and observing the reaction of security personnel (e.g., the time it takes to respond to an incident or the routes taken to a specific location).

f) Unauthorized personnel accessing IT spaces linked to security plan functions.

g) Unsuccessful attempts to access telecommunication, computer, and network systems linked to security plan functions.

vi. The Coast Guard recognizes that the cyber domain includes countless malicious but low-level events that are normally addressed via standard anti-virus programs and similar protocols. Operators should only report events that are out of the ordinary in terms of sophistication, volume, or other factors which, from the operator’s perspective, raise suspicions.

C. Reporting Procedures

i. Report SA and BoS to the National Response Center (NRC) at 1-800-424-8802. Facility and vessel operators may also make reports directly to the local COTP; however, this does not relieve an owner or operator from the requirements of 33 CFR part 101.305. Facility personnel and mariners are also encouraged to report suspicious UAS activity to Americas Waterway Watch (AWW) (877)-24-WATCH (877-249-2824), and the DHS "See Something, Say Something" campaign.

ii. When reporting security incidents to the NRC, they will request the following information:

a) Reporting source information;

b) Incident location, including physical address;

c) Type of facility or vessel; and

d) Brief summary of activity and its impact.

iii. The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. For cyber incidents that do not also involve physical or pollution effects, the Coast Guard allows reporting parties to call and report the incident to the NCCIC in lieu of the NRC, as the NCCIC may be able to provide technical assistance to the reporting party. The NCCIC can be reached at (888) 282-0870. It is imperative that the reporting party inform the NCCIC that they are a Coast Guard regulated entity in order to satisfy the reporting requirements of 33 CFR part 101.305. The NCCIC will forward the report electronically to the NRC, who will notify the appropriate COTP.

iv. Reporting cyber incidents in this manner, including notifying the NCCIC that the reporting source is regulated by the Coast Guard, meets Coast Guard regulatory requirements. Note that this is applicable for only a cyber incident; if there are other factors involved, such as pollution or a physical breach of security, operators must report the incident directly to the NRC.

v. The purpose of reporting is to promote security, and in some cases it may therefore be appropriate for an organization to provide only the most basic information to the NRC and to provide further details directly to the COTP, Federal Bureau of Investigation (FBI), and other organizations with a need to know. The details of any security vulnerabilities revealed by the event need not be discussed during an initial report. The Coast Guard will work with the reporting source and with other appropriate authorities to assess and respond to the report.

D. Other Critical Infrastructure and Cyber Incident Resources

i. While not required by U.S. Coast Guard regulations, vessel and facility operators, port authorities, and others may wish to discuss their cyber incidents with the NCCIC including ICS-CERT for cyber incidents related to industrial control systems. Depending on the situation, the NCCIC may be able to provide assistance. ICS-CERT has also published best practices that can be found at https://ics-cert.us-cert.gov/Recommended-Practices.

ii. The FBI InfraGard program provides members of the critical infrastructure community a means to share information to prevent, protect, and defend against hostile acts against Critical Infrastructure and Key Resources.

iii. The National Suspicious Activity Reporting (SAR) Initiative provides information and resources related to SA reporting. The SAR Initiative is a joint collaborative effort by DHS, the FBI, and state, local, tribal and territorial law enforcement partners. Note that this is a source of information, not a reporting center.

iv. The U.S. Coast Guard encourages vessel and facility operators to participate in their local AMSC. These committees are the best place to collaborate with colleagues at the port level for security and information sharing, including the resources, services and capabilities of other federal, state, local and private sector partners. To learn more about the AMSC, contact your local Coast Guard COTP.

v. To promote clear communications, this policy letter includes a glossary of common cyber terms. A more complete lexicon, along with other information on cyber security, suspicious activity, and AMSC, is available on the Coast Guard's Homeport website.

4. Disclaimer. This policy is not a substitute for applicable legal requirements, nor is itself a rule. It provides operational guidance for U.S. Coast Guard personnel and the maritime industry. It is does not impose legally binding requirements on any party outside of the U.S. Coast Guard.

5. Questions concerning this policy should be directed to the U.S. Coast Guard Office of Port and Facility Compliance (CG-FAC) at (202) 372-1132.

#

Enclosure: (1) Glossary of Terms

Glossary of Terms[i]

Access – The ability to make use of any information system (IS) resource (Reference (d)).

Adversary – An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities (Reference (d)).

Breach of Security – An incident that has not resulted in a Transportation Security Incident (TSI) but in which security measures have been circumvented, eluded, or violated. (33 CFR, Subchapter H, Maritime Security)

Cyber Effects – The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (U.S. Coast Guard Cyber Strategy, June 2015)

Cyber Event – A cybersecurity change that may have an impact on organizational operations, including mission, capabilities, or reputation (Reference (e)).

Cyber Incident – Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein (Reference (d)).

Cybersecurity – The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (U.S. Department of Homeland Security. National Infrastructure Protection Plan, 2013)

Cybersecurity Breach – Unauthorized access to data, applications, services, networks and/or devices, by-passing their underlying security mechanisms. A cybersecurity breach that may rise to the level of a reportable Maritime Transportation Security Act (MTSA) security breach occurs when an individual, an entity, or an application illegitimately enters a private or confidential Information Technology perimeter of a MTSA-regulated facility or vessel, Maritime Critical Infrastructure/Key Resources, or industrial control system such as Supervisory Control and Data Acquisition systems, including but not limited to terminal operating systems, global positioning systems, and cargo management systems. (U.S. Coast Guard Atlantic Area Commanders Intent: Advancing Knowledge of Cyber Security Trends and Threats to the Maritime Transportation System (MTS), 4 November 2013; U.S. Coast Guard Pacific Area Commanders' Intent: Cyber Security and the Maritime Transportation System (MTS), 8 November 2013)

Cyber Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction,

disclosure, modification of information, and/or denial of service (Reference (d)).

Insider Threat – An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and /or denial of service (Reference (d)).

Intrusion – Unauthorized act of bypassing the security mechanisms of a system (Reference (d)).

Intrusion Detection Systems (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations) (Reference (d)).

Malicious Cyber Activity – Activities, other than those authorized or in accordance with U.S. law, that seek to compromise the confidentiality, integrity, or availability of computers, information or communications systems, physical or virtual infrastructure controlled by computers or information systems, or information thereon. (U.S. Coast Guard Cyber Strategy, June 2015)

Outside Threat – An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service (Reference (d)).

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means (Reference (d)).

Risk Mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (Reference (d)).

Network defense – The programs, activities, and the use of tools necessary to facilitate them conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting 1) that computer, network, or system; 2) data stored on, processed on, or transiting that computer, network, or system; or 3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners. (U.S. Coast Guard Cyber Strategy, June 2015)

Recovery Procedures – Actions necessary to restore data files of an information system and computational capability after a system failure (Reference (d)).

Suspicious Activity – Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity (Reference (c)).

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invoke the program (Reference (d)).

Unauthorized Access – Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use (Reference (d)).

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk (Reference (d)).

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself (Reference (d)).

Zombie – A program that is installed on a system to cause it to attack other systems (Reference (d)).

[i] This glossary is primarily meant to provide cyber related definitions that are not listed in 33 Code of Federal Regulations part 101.105.