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

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington DC 20593-7318
Staff Symbol: CG-FAC

NVIC 02-24, CH 1
November 12, 2025

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 02-24, Change 1

Subj: REPORTING BREACHES OF SECURITY, SUSPICIOUS ACTIVITY, TRANSPORTATION SECURITY INCIDENTS, AND CYBER INCIDENTS

Ref: (a) Title 33, Code of Federal Regulations, Subchapter H (Maritime Security)
(b) 46 United States Code (USC) § 70103(c)(3)(A)
(c) Title 33, Code of Federal Regulations, Part 6 (Protection and Security of Vessels, Harbors, Ports, and Waterfront Facilities)
(d) Assessment and Review of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Indicators
(e) Executive Order 14116 on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) provides guidance for complying with reporting requirements for a breach of security (BOS), suspicious activity (SA), transportation security incident (TSI), cyber incident, and reportable cyber incident (RCI). The cyber incident guidance in this NVIC supports the reporting requirements in Title 33, Code of Federal Regulations, Part 6 (33 CFR 6) that applies to any vessel, harbor, port, or waterfront facility (hereafter referred to as MTS stakeholders). The BOS, SA, and TSI guidance in this NVIC supports the reporting requirements applicable to Maritime Transportation Security Act of 2002 (MTSA)-regulated entities subject to 33 CFR 101.305. The RCI guidance in this NVIC supports the reporting requirements in 33 CFR 101.620(b)(7).

2. BACKGROUND.

   a. Under 33 CFR 101.305, MTSA-regulated entities are required to report a BOS, SA, and TSI to the Coast Guard. Previously, CG-5P Policy Letter 08-16 provided guidance as well as specific examples of a BOS and SA, including those involving computer systems and networks, to help industry meet MTSA reporting requirements. That Policy Letter was superseded by NVIC 02-24, which added guidance on reporting cyber incidents as required by Reference (c).

   b. On February 21, 2024, the Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States amended 33 CFR 6. Among other provisions, it added a definition for “cyber incident” and created a requirement to immediately report evidence of an actual or threatened cyber

incident involving or endangering any vessel, harbor, port, or waterfront facility to the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA) (for any cyber incident), and the Coast Guard Captain of the Port (COTP). Notably, the applicability of 33 CFR 6 does not include Outer Continental Shelf (OCS) facilities. The broad applicability of 33 CFR 6 and the new definition of a cyber incident created a partial overlap with MTSA reporting requirements.

c. On July 16, 2025, the Coast Guard updated its maritime security regulations by establishing minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities required to have a security plan under 33 CFR parts 104, 105, and 106. Among other provisions, it added a definition for "reportable cyber incident" and created a requirement in 33 CFR 101.620 for entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1, to report all RCIs to the National Response Center (NRC).

3. DIRECTIVES AFFECTED: NVIC 02-24, published February 21, 2024, is cancelled and replaced by NVIC 02-24, Change 1. Change 1 provides updated guidance to comply with References (a) through (e).

4. ACTION. COTP, Area Maritime Security Committees (AMSC), MTS stakeholders, and MTSA-regulated entities may use this guidance when considering whether a report is required for a BOS, SA, TSI, RCI, or cyber incident. This NVIC will be distributed by electronic means only. It is available by accessing the Coast Guard's Maritime Industry Cybersecurity Resource Center website.

a. In accordance with Reference (a), An owner or operator of a vessel, facility, or OCS facility that is required to maintain an approved security plan in accordance with MTSA (i.e., MTSA-regulated entities) and its implementing regulations in Reference (a), shall, without delay, report activities that may result in a TSI to the NRC, including BOS or SA as required by 33 CFR 101.305. The purpose of this requirement is to provide the Coast Guard with an opportunity to understand and respond to potential or actual threats to the port area and to assess the adequacy of security plans to prevent a TSI. Additionally, in accordance with Reference (b), the security plan 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 communication procedures within FSPs throughout their area of responsibility.

b. In accordance with Reference (c), Evidence of sabotage, subversive activity, or an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, including any data, information, network, program, system, or other digital infrastructure thereon or therein, shall be reported immediately to the FBI, CISA (for any cyber incident), and to the COTP, or to their respective representatives, per 33 CFR 6.16-1. The purpose of this requirement is to provide the Coast Guard, FBI, and CISA, the opportunity to understand and respond to potential or actual threats to the MTS and determine appropriate actions.

c. OCS facilities are not subject to Reference (c) and are therefore not required to report "cyber incidents" per 33 CFR 6.16-1. However, OCS facilities *are* required to report RCIs in accordance with 33 CFR 101.620(b)(7). Because there is overlap between the term "cyber incident" used in 33 CFR Part 6 and "reportable cyber incident" used in 33 CFR Part 101, the 33 CFR 101.620 obligation to report a "reportable cyber incident" ("RCI") only applies to entities who are not subject to 33 CFR Part 6 (i.e., OCS facilities).

d. The maritime industry continues to expand its use of networked technology, which creates efficiencies but also increases threats and vulnerabilities to MTS stakeholders and MTSA-regulated entities 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 has a network or computer nexus. Maintaining the security of these systems, including reporting cyber incidents and RCIs, is vital to maintaining the security of the MTS.

e. Plausible terrorist attack scenarios include combined cyber and physical incidents. MTS stakeholders, including those that are MTSA-regulated, should consider this possibility when evaluating a security incident, including the possibility that a cyber incident is a precursor to a physical attack, or an attempt by malicious actors to identify weaknesses or to plan for later attacks.

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

5. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The Office of Environmental Management, Commandant (CG-SHORE-V) reviewed this NVIC and the general policies contained within and determined that this policy falls under the Department of Homeland Security (DHS) categorical exclusion A3. This NVIC will not result in any substantial change to existing environmental conditions or violation of any applicable federal, state, or local laws relating to the protection of the environment. It is the responsibility of the action proponent to evaluate all future specific actions resulting from this policy for compliance with the National Environmental Policy Act (NEPA), other applicable environmental requirements, and the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 (series).

b. This NVIC will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this NVIC must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

6. RECORDS MANAGEMENT CONSIDERATIONS. This NVIC has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not create significant or substantial change to existing records management requirements.

7. FORMS/REPORTS. None.

8. DISCLAIMER. This NVIC is intended only to provide clarity regarding existing requirements under the law and regulation. It does not change any legal requirement and does not impose new requirements on the public. It provides operational guidance for U.S. Coast Guard personnel and the maritime industry.

9. QUESTIONS. Questions concerning this policy should be directed to the U.S. Coast Guard Office of Port and Facility Compliance (CG-FAC) at MTSCyberRule@uscg.mil.

W. R. Arguin,
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Policy

Encl: (1) Reporting Guidance
(2) Glossary of Terms

Reporting Guidance

1. DISCUSSION. The following criteria describe U.S. Coast Guard requirements and amplifying guidance for reporting BOS, SA, TSI, RCIs, and cyber incidents. No description could cover all possible incidents and events. When in doubt about whether a situation meets the reporting criteria, affected entities should make a report as described in 33 CFR 101.305, 33 CFR 101.620, and 33 CFR 6.16-1, as applicable.

   a. Cyber Incident and RCI

      (1) **This section applies to all MTSA-regulated entities and MTS stakeholders.**

      (2) To harmonize cyber incident (as the term is used in 33 CFR Part 6) and RCI (as the term is used in 33 CFR Part 101) reporting requirements to the U.S. Coast Guard, MTSA-regulated entities and MTS stakeholders must report those incidents that lead to or, if still under investigation, could reasonably lead to any of the following:

         (a) Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system;

         (b) Disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death;

         (c) Disclosure or unauthorized access directly or indirectly of nonpublic personal information of a significant number of individuals;

         (d) Other potential operational disruption to critical infrastructure systems or assets; or

         (e) Incidents that otherwise may lead to a transportation security incident as defined in 33 CFR 101.105.

      (3) The cyber domain includes countless malicious but low-level events, such as routine spam, phishing attempts, and other nuisance events that are normally addressed by standard anti-virus programs and cyber hygiene protocols. Additionally, accidental violations of acceptable use policies, such as plugging in an unauthorized portable hard drive or memory stick, is not considered a cyber incident. MTS stakeholders should report events that are out of the ordinary in terms of sophistication, volume, or other factors which, from the operator's perspective, raise suspicions and may result in a TSI.

   b. Breach of Security (BOS)

      (1) **This section applies to all MTSA-regulated entities.**

(2) Reference (a) defines a BOS as, "an incident that has not resulted in a TSI, in which security measures have been circumvented, eluded, or violated."

(3) BOS incidents may include, but are not limited to, any of the following:

(a) Unauthorized access to restricted or secure areas as designated in the security plan;

(b) Unauthorized circumvention of security measures, such as purposefully disabling a security camera, piggybacking through a vehicle gate without clearance, or a breach of a perimeter fenceline;

(c) A cyber incident or RCI that involves unauthorized access to or degrades IT or OT systems that execute physical security functions required in the security plan or that could otherwise result in a TSI.

c. Suspicious Activity (SA)

(1) **This section applies to all MTSA-regulated entities.**

(2) Reference (a) describes SA as "an activity that may result in a TSI." Reference (d) defines SA as, "observed behavior reasonably indicative of pre-operational planning related to terrorism or criminal activity."

(3) SA may include, but is not limited to, any of the following:

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

(b) Unauthorized personnel physically accessing spaces or equipment involving an information system;

(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) Unusual behavioral patterns, such as:

i. Walking slowly in a deliberate fashion towards a potential target;

ii. Inappropriately dressed (for example, wearing excessive clothing as to conceal something, or looking out of place);

iii. Not responding to verbal interaction;

iv. Excessive nervousness or "doomsday" talk;

v. Excessive questions;

vi. Lack of photo identification;

vii. Agitation or rage;

viii. Picture taking, especially if the suspect has been asked earlier not to take photos;

ix. Note taking or drawing;

x. Taking measurements; or,

xi. Attempting to access unauthorized areas.

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

i. Reconnaissance and surveillance activities, indicated by repeated activities at a particular place and time (for example, fly-overs, hovering at low altitudes, and prolonged time on station); or,

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

(g) Cybersecurity-related SA should be distinguished from nuisance events that are part of the normal internet landscape, such as persistent scanning of networks, spam emails, and similar unsophisticated events. Nuisance events should be monitored for signs of escalation in volume, persistence, or sophistication that could be indicative of malicious efforts that should be reported.

d. Transportation Security Incident (TSI)

(1) **This section applies to all MTSA-regulated entities.**

(2) Reference (a) defines TSI as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area."

(3) Cyber incidents that clearly target or otherwise affect business or administrative systems, even without directly affecting operational technology or industrial control systems that result in a transportation system disruption or economic disruption may still be considered a TSI depending on the potential or resulting impact.

e. Reporting Procedures

(1) BOS or SA

(a) MTSA-regulated entities must report a BOS or SA to the National Response Center (NRC), without delay, at 1-800-424-8802. MTSA-regulated entities may also make reports directly to the local COTP; however, this does not relieve an owner or operator from the requirement to notify the NRC in accordance with 33 CFR 101.305.

(2) TSI

(a) MTSA entities regulated under 33 CFR 104 or 105 shall, without delay, report a TSI to the local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the NRC.

(b) MTSA entities regulated under 33 CFR 106 shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the NRC.

(3) Cyber Incidents

(a) **For the purposes of cyber incident reporting in accordance with reference (c), a notification, without delay, directly to the NRC is strongly recommended and fulfills the requirement to notify the COTP. Additionally, a notification directly to the NRC will be immediately forwarded to the FBI CyWatch at cywatch@fbi.gov which the FBI will accept as a report, and therefore fulfills both the requirement to report to the COTP and the FBI.**

(b) **A separate report must be made to CISA at (844) Say-CISA (844-729-2472),** SayCISA@cisa.dhs.gov **or at** CISA Service Portal

(c) If a maritime stakeholder believes that the cyber incident may have occurred in or may have an impact in more than one COTP zone, this shall be relayed to the NRC in the report to ensure the incident information is relayed to the appropriate COTPs.

(4) Reportable Cyber Incidents (RCI)

(a) Regulated entities not subject to 33 CFR 6, such as OCS facilities regulated under 33 CFR 106, must report all RCIs without delay to the NRC in accordance with 33 CFR 101.620.

(b) To minimize duplicative reporting from the same entity, the requirement to report under 33 CFR 101.620 does not apply if the entity has reported the cyber incident to the Coast Guard pursuant to 33 CFR 6.16-1.

(5) When reporting security incidents, owners and operators should be prepared to provide the following information:

(a) Reporting source information;

(b) Incident location, including physical address;

(c) Type of facility, vessel, port, or harbor; and,

(d) Brief summary of activity and its impact or potential consequence(s).

(6) 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, COTP, FBI, CISA, and other organizations with a need to know. The details of any security vulnerabilities revealed by the event do not need to 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.

f. Specific Reporting Cases

(1) Reporting BOS and SA in the Cruise Ship Terminal Screening Program:

(a) As part of the Cruise Ship Terminal Screening Program, 33 CFR 105.515 provides regulations pertaining to a Prohibited Items List (PIL). The PIL consists of dangerous substances and devices that the Coast Guard prohibits onboard any cruise ship through terminal screening operations. The owner or operator of a cruise ship terminal must obtain the PIL from the Coast Guard and the list must be present at each screening location during screening operations. If any of the prohibited items are found by screeners during the security screening, then that incident would be classified as SA. However, if any of the prohibited items are found after security screening procedures, that indicates security measures were likely circumvented and would be classified as a BOS.

(b) Loose ammunition in the absence of a firearm found during the screening process is not considered SA for the purposes of reporting to the NRC unless consultation with local law enforcement indicates otherwise. Any amount of ammunition discovered to be missed by screening procedures will result in a BOS and must be reported to the NRC. Ammunition found during the screening process should be documented by the facility owner/operator as a security threat per 33 CFR 105.225(b)(6) and be treated according to local law enforcement practices per 33 105.515(d).

(2) Reporting BOS and SA for Unauthorized Unmanned Aircraft System (UAS) Activity:

(a) All unauthorized UAS activity over a MTSA-regulated facility or vessel should be closely observed, documented and reported to local law enforcement and to the NRC as SA. If the UAS lands or crashes on or into a regulated facility or vessel, or the UAS operates below the height of the perimeter security fencing at a facility, the incident shall be considered a BOS.

(b) The Coast Guard highly recommends that the Facility Security Officer (FSO) or the Vessel Security Officer (VSO) also report the incident to local law enforcement if the UAS is not following Federal Aviation Administration (FAA) enforceable regulations. Before reporting the incident, review FAA regulations to make sure there is a violation. In some cases, flying a UAS over a MTSA-regulated facility or vessel is not in violation of FAA regulations. Examples of

violations of FAA regulations are hazardous operations (careless or reckless), operations over human beings, and operation in a controlled airspace. Consult the FAA Facility Maps to identify controlled airspace in the COTP Zone. FSOs/VSOs can report the violation(s) to local law enforcement or the FAA local flight standards district office.

g. Other Critical Infrastructure and Cyber Incident Resources

(1) Every Coast Guard Sector, District, and Area office has a Marine Transportation System Specialist - Cyber (MTSS-C) position serving as a primary advisor for their respective commands on all matters related to maritime cybersecurity, risk management, and incident response. These MTSS-Cs also serve as liaisons to maritime industry and promote resilience through assisting in the implementation of policies, enhancing cyber threat awareness, and connecting stakeholders with additional resources. To get in touch with an MTSS-C, contact the local COTP/Sector office.

(2) The U.S. Coast Guard Cyber Protection Team(s) (CPT) are the Coast Guard's deployable units responsible for offering cybersecurity capabilities to Marine Transportation System (MTS) partners. To discuss capability details and what a CPT can do for your organization, contact the team at MaritimeCyber@uscg.mil for a tailored introduction. Request are prioritized based on the time, nature, and criticality. Incident Response support should be communicated via the National Response Center (800-424-8802).

(3) In addition to the reporting requirements of 33 CFR 101.305, 33 CFR 101.620, and 33 CFR 6.16-1, MTS stakeholders and MTSA-regulated entities may be subject to additional reporting requirements issued by other agencies such as CISA or other federal, state, local, tribal and territorial entities.

(a) CISA Central is CISA's hub for tracking threats and emerging risks to our nation's critical infrastructure and are a resource for critical infrastructure partners and stakeholders. CISA Central can be reached 24x7 at SayCISA@cisa.dhs.gov or (844) Say-CISA (844-729-2472).

(b) CISA offers a wide range of free products and services to support the maritime community's cybersecurity security risk management efforts. A full list of service offerings and resources with additional details can be found on CISA's Resources and Tools website.

(4) The InfraGard program is a unique partnership between the FBI and the private sector for the protection of the Nation's critical infrastructure and the American people. It connects critical infrastructure owners, operators, and stakeholders with the FBI to provide education, networking, and information sharing on security threats and risks.

(5) 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.

(6) The U.S. Coast Guard encourages MTS stakeholders and MTSA-regulated entities to participate in their local AMSC. These committees are a vital opportunity 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 the local COTP.

#

Glossary of Terms

Industrial Control System (ICS) — An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

Security Threat – A potential for a violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

Unauthorized Access — A person gains logical or physical access without permission to a cyber or physical resource.