Transport Canada Transports Canada

MARINE SECURITY OPERATIONS BULLETIN

ISSN 3110-2250 **No: 2026-002**

REPORTING REQUIREMENTS CONCERNING MARINE SECURITY THREATS, BREACHES, AND INCIDENTS

PURPOSE:

This bulletin reminds stakeholders subject to the Marine Transportation Security Regulations (MTSR) and the Domestic Ferries Security Regulations (DFSR) of their obligation to report all security threats, breaches and incidents to the National Transport Canada Situation Centre (TCSC) as soon as possible. Reporting to TCSC fulfills the requirement to report to the Minister of Transport. This bulletin also clarifies reporting procedures and the definitions of security threats, breaches and incidents.

This bulletin should be used in conjunction with MSOB 2026-003 which provides guidance on reporting cyber security threats, breaches and incidents, as well as MSOB 2026-004 on suspicious activity reporting. This bulletin supersedes previous guidance related to the mandatory reporting of security threats, breaches and incidents, including MSOB 2014-001.

DEFINITIONS:

Security Threat: *Any suspicious act or circumstance that could compromise the security of a vessel, marine facility, port or interface.*

Security Breach: *Violation of security regulations, measures, rules or procedures that does not result in a security incident.*

Security Incident: *An event during which the security of a vessel, marine facility or port is compromised.*

Threats, breaches and incidents are not restricted by the means by which they occur and include both physical and cyber-related events. For more specifics regarding cyber related threats, breaches and incidents, please refer to MSOB 2026-003.

BACKGROUND:

Effective October 2, 2012, TC Marine Security Operations centralized the reporting of security threats, security breaches, and security incidents to the National TC Situation Centre (TCSC) telephone reporting line. This reporting number replaced all other Regional and National Marine Security emergency contact numbers originally published in MSN 2007-001. At that time, regulated stakeholders were requested to formally update the threat, breach and security incident reporting procedures and contact numbers in their security plans to reflect the change and submit their amended security plans for approval by TC.

ffdsfds

Transport Canada Transports Canada

In order to stay ahead of evolving threats, it is important that Canada's marine security regime be proactive, risk-based, and responsive. Consistent and timely reporting of security threats, breaches, and incidents, in accordance with the regulations and this policy directive, is necessary to ensure rapid information distribution to TC personnel responsible for regulatory oversight and to facilitate timely, whole-of-government response coordination to security events.

TC uses information from reports of security threats, breaches, and incidents to identify trends and patterns, make decisions when addressing potential threats that may be identified, and to inform port, facility, and vessel security assessments.

Directive:

1. **Port administrations, marine facilities, and ferry facilities**

   In accordance with the MTSR and the DFSR, stakeholders are required to report all security threats and security incidents that occur at a marine facility, ferry facility, port, or at an interface between a vessel and a marine or ferry facility, or between vessels. These reports must be made as soon as possible to the appropriate law enforcement agencies, the Minister of Transport, and, where applicable, the relevant port administration, to ensure that timely investigations and response actions can be undertaken.

   Security breaches must also be reported as soon as possible after they occur; however, breaches are only required to be reported to the Minister and the port administration, if applicable. Timely and accurate reporting supports coordinated response efforts, regulatory oversight, and the ongoing assessment of risks to Canada's marine transportation system.

2. **Canadian flagged regulated vessels and ferries**

   Security threats and incidents involving vessels or ferries subject to the MTSR or DFSR must be reported as soon as possible to the vessel's master, the Company Security Officer (CSO), the appropriate law enforcement agencies, the Minister of Transport, and, when applicable, the port administration to enable an investigation.

   These reporting requirements apply for Canadian-flagged vessels subject to the MTSR that may operate in foreign waters, regardless of whether they are in Canadian or foreign waters.

   Regardless of the vessel's location, any security breaches on Canadian-flagged vessels or ferries governed by the MTSR or DFSR must be reported immediately to the Minister and, if applicable, the port administration. Any security threats and security incidents occurring on Canadian-flagged vessels or ferries governed by the MTSR or DFSR must be reported to the master, the company security officer, the appropriate law enforcement agencies, the Minister and, if applicable, the port administration. Timely reporting ensures that Transport Canada and partner agencies can assess risk, support response actions, and maintain oversight of marine transportation security.

Transport Canada Transports Canada

3. **Security plan amendments**

All regulated stakeholders shall review their security plans and related security documentation and, where necessary, formally amend them to reflect on these mandatory reporting requirements in order to maintain compliance with the MTSR and the DFSR.

Stakeholders must submit all amendments to their security plans to their respective Transport Canada Regional Marine Security Office for review and approval.

PROCEDURES

To meet the mandatory reporting requirements under the MTSR and the DFSR, stakeholders must report all security threats, breaches and incidents directly to the National Transport Canada Situation Centre (TCSC), which fulfills the requirement to report to the Minister of Transport.

All security threats, breaches and incidents shall be reported directly to the National TCSC at:

1-888-857-4003 (toll-free within Canada/U.S.) or

1-613-995-9737 (all other areas)

This reporting requirement is in place 24 hours a day, 7 days a week.

Follow up reports or documentation may be emailed to Sitcen@tc.gc.ca

Reminder: all threats and incidents must also be reported to:

- **Appropriate law enforcement organization; and,**
- **Port Administration (if applicable)**

Any event that meets the definition of a security threat, security breach, or security incident under either the MTSR or the DFSR must be reported to the National TCSC as soon as possible after it occurs. Failure to report may result in enforcement action.

It is recognized that stakeholders may need to take immediate action to respond to a threat, breach, or incident. In such cases, stakeholders must contact the National TCSC to report the event at the earliest possible opportunity after immediate actions have been taken to preserve life, safety, and security.

For greater clarity, “as soon as possible” means at the first opportunity after an event occurs, without undue delay. To ensure ongoing compliance with the Regulations, stakeholders must not wait until the next business day to report a security threat, breach, or incident.

To determine whether an event requires reporting to Transport Canada, stakeholders should consider whether:

- Any established security policy, safeguard, measure, or procedure was circumvented, regardless of whether the event was intentional or accidental, and regardless of whether the

ffdsfds

security of a vessel, facility, port, or marine installation was affected;

- The event did or has the potential to threaten or affect the integrity of the security posture of a port, facility, vessel, ferry, or ferry facility, or the integrity of assets and infrastructure;
- The event could impact other vessels, facilities, or ports;
- The event could impact national security or the general security and continued functioning of the marine transportation system and its infrastructure;
- The event requires liaison or coordination with the regulatory or security community;
- The event may require the attendance of a Transport Canada Marine Security Inspector to observe or provide regulatory guidance;
- The event has triggered the implementation of alternate security arrangements; or
- The event has otherwise affected the ability of a port, facility, vessel, or ferry to fully implement its security plan.

A non-exhaustive list of examples of events triggered by security threats, breaches, and incidents is provided in Annex A. **This list is intended as guidance only**. Any event that meets the definition of a security threat, breach, or incident must be reported as soon as possible, without undue delay.

QUESTIONS

If there is any uncertainty about whether an event requires reporting, stakeholders are strongly encouraged to contact the National TCSC and submit a report.

Any comments, suggestions or concerns can be addressed to the Director, Marine Security Operations by e-mail at dirops.marsec-surmar@tc.gc.ca.

Ryan, Aiden
Digitally signed by Ryan, Aiden
Date: 2026.06.11 11:53:53 -04'00'

Aiden Ryan
Director
Marine Security Operations

Transport Canada Transports Canada

ANNEX A

This is a non-exhaustive list of examples of security incidents, threats and breaches that must be reported as soon as possible to Transport Canada. The categorization of examples is for guidance only, and the appropriate classification of an event may vary depending on the specific circumstances.

Security incidents

- Any security incident (physical or cyber) that has affected the security of personnel, cargo, a vessel, ferry, marine or ferry facility, an interface between vessels or between a vessel and a marine or ferry facility or another vessel;
    - MSOB 2026-003 has further examples of reportable events related to cybersecurity

- Any activity that compromises the confidential nature of sensitive information whether physical or cyber;

- Any security event that has or may cause disruption to commercial shipping;

- Any discovery of an unsecured facility / unprotected restricted area (or restricted area two) where upon investigation it is determined that the security of personnel, a vessel, ferry, facility, marine facility, an interface between vessels or between a vessel and a marine facility or another vessel has or could have been compromised;

- Any discovery of suspicious packages at a marine or ferry facility, port, on board a Canadian vessel or on board an interfacing vessel;

- Any discovery of suspicious persons/photography and/or drone activity at a marine or ferry facility, port, on board a Canadian vessel or on board an interfacing vessel;
    - MSOB 2026-004 has further examples of reportable events related to suspicious activities

- Any loss, theft or damage (physical or cyber) to marine facilities or infrastructure that affect the security of a facility, port or vessel;

- All reports of the use of counterfeit, stolen or otherwise unauthorized use of restricted area or restricted area two passes;

- All events where there is an explosion, armed attack, hijacking or hostage taking on board a vessel, at a marine or ferry facility, port or adjacent marine infrastructure;

- Any violent crimes or intimidation associated to a vessel, ferry, marine or ferry facility or a port;

- Any system tampering or failure, electrical, cyber or otherwise that has affected a security system, safeguard, measure or procedure related to a vessel, a marine facility or port (also consider interruptions to GPS-based devices such as: navigation, control and safety systems, and to Industrial Control Systems (ICS) that support cargo handling equipment and tracking systems, general terminal operations, port security access controls, dam and lock controls, and other water or shore based systems or objects that directly support safe and secure vessel operation and navigation);

ffdsfds

- Any event that requires alternate security arrangements to be put in place;
- Any vessel collision, sinking, grounding, or oil or noxious substance spill resulting from a security incident;
- Any event where the security of cargo, containers, certain dangerous goods, or hazardous and noxious substances on board vessels, in facilities or ports has been compromised;
- Any event involving the intervention of a peace officer on board a vessel, ferry or at a marine facility, ferry facility or a port;
- Any discovery of a weapon at a port, facility, or on board a vessel or facility;
- Any loss of life as a result of a security event on board a vessel, at a marine facility or port;
- Any fire on board a vessel, at a marine or ferry facility or at a port resulting either from a security incident or that could affect the security of a marine or ferry facility, port or vessel.

Security breaches

- Any violation of security regulations, measures, rules or procedures that does not result in a security incident, including but not limited to:
    - Any intrusion or attempted intrusion by any unauthorized person on a vessel, ferry, a facility, a port or in a restricted or restricted area two, including but not limited to:
        - Bypassing designated screening check points or access control points; and
        - Not providing proper credentials.
    - The discovery of an unauthorized person in a restricted area, or a restricted area two.
- Stealing or diverting something associated with the security of a facility/infrastructure/vessel, or possessing actual or fraudulent facility/infrastructure/vessel specific articles (uniforms, keys, badges, identification, technology, documents, which are proprietary to the facility);
- Presenting false or misusing documents or identification to misrepresent one's identity, affiliation, or to cover possible unauthorized or illicit activity;
- Interactions with, or challenges to installations, vessels, personnel, or systems that reveal physical, personnel or cyber security capabilities;
- Tampering with physical or environmental security controls such as fences, barriers, doors, gates, locks, monitoring or detection systems, lighting, HVAC systems, power protection or water and fire protection;
- The loss, theft, or damage of property where it was necessary to bypass security controls, procedures or systems and the loss or theft did not affect the security posture of the vessel, port or facility;

ffdsfds

- Cyber events where established system controls were bypassed, but did not result in the loss of sensitive information or system failure (unauthorized attempts to change system hardware, firmware or software; unauthorized attempts to access the network, unauthorized use of the system/network); and

- Interactions with, or challenges to installations, personnel, systems or cargo that reveal physical, personnel or cyber security capabilities or vulnerabilities,

Security Threats

- Any special interest events or work stoppages (real or planned) which pose a threat against people, vessels, or facilities or marine infrastructure or could result in the disruption of the marine transportation system;

- Any threat, real or implied, against a vessel, ferry, marine or ferry facility, port or adjoining marine infrastructure;

- Receipt of any information concerning unauthorized weapons, dangerous substances and devices, suspicious packages, or equipment intended for use against persons, vessels or marine or marine facilities' or the transportation system;

- Any event or circumstance that leads to an increase in Marsec Level by any Canadian vessel subject to the MTSR or DFSR anywhere; and

- Any event that may cause a disruption or that threatens disruption to commercial shipping.

When in doubt, report it.