Transport Canada Transports Canada

MARINE SECURITY OPERATIONS BULLETIN

No: 2014- 001

CLARIFICATION OF TRANSPORT CANADA (TC) MARINE SECURITY MANDATORY THREAT, BREACH AND INCIDENT REPORTING REQUIREMENTS

THIS MARINE SECURITY OPERATIONS BULLETIN (MSOB) REPLACES MARINE SECURITY NOTIFICATION (MSN) 2012-005 *CHANGE OF TRANSPORT CANADA MARINE SECURITY NATIONAL EMERGENCY PHONE NUMBER.*

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 previously 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.

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 facilitate timely whole of government response coordination to security events.

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

PURPOSE:

This MSOB serves as a reminder to stakeholders subject to the Marine Transportation Security Regulations (MTSR) or the Domestic Ferries Security Regulations (DFSR) of the regulatory obligation to report all security threats, breaches and incidents as soon as possible to the National TCSC after they have occurred. It also reinforces and clarifies reporting procedures and definitions of security threat, security breach and security incident definitions.

DEFINITIONS:

Security threats, security breaches and security incidents are defined as follows:

Security threat: Any suspicious act or circumstance that could threaten the security of:

- A vessel or ferry;
- An interface between vessels or ferries;
- An interface between a vessel and a marine facility or between a ferry and ferry facility;
- A marine or ferry facility; or
- A port administration.

Security breach: A violation of security regulations, measures, rules or procedures that does not result in a security incident.

Note: Currently, the MTSR uses the term breach of security while the DFSR uses security breach. Although there is a difference in terminology between the MTSR and the DFSR, the concept and definition is similar. As the MTSR is proposed to be amended to reflect the same wording and definition as used in the DFSR, this document uses the term security breach. For clarity any reference to security breach in this document also refers to breach of security as currently outlined in the MTSR.

Security incident: An incident that has affected the security of:

- A vessel or ferry;
- An interface between vessels or ferries;
- An interface between a vessel and a marine facility or between a ferry and ferry facility;
- A marine or ferry facility; or
- A port administration.

DIRECTIVE:

1. Port administrations, marine facilities, and ferry facilities

In accordance with the MTSR and the DFSR, stakeholders shall report all security threats and incidents occurring at a marine facility, a ferry facility, a port, or an interface between a vessel and a marine or ferry facility or another vessel as soon as possible to appropriate law enforcement agencies, the Minister and, if applicable, the port administration, as soon as possible after they occur so that an investigation can be conducted. Security breaches must also be reported as soon as possible after they occur, but must only be reported to the Minister.

2. Canadian flagged regulated vessels and ferries

With respect to vessels and ferries subject to the provisions of the MTSR or DFSR, security threats and security incidents shall be reported to the master, the company security officer, the appropriate law enforcement agencies, the Minister and, if applicable, the port administration, as soon as possible after they occur so that an investigation can be conducted. For Canadian flagged vessels subject to the MTSR's that are operating in foreign waters, these reporting requirements shall be met regardless of the location of the vessel.

Security breaches that occur aboard a Canadian flagged vessel or ferry subject to the MTSR or DFSR shall also be reported to the Minister as soon as possible after they occur, regardless of the location of the vessel.

3. Procedures for mandatory regulatory reporting to the Minister

For the purpose of reporting security threats, breaches and incidents, in accordance with the MTSR and the DFSR, contacting the National TCSC fulfils stakeholder obligations to report to the Minister.

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 with a carbon copy to your TC regional marine security office.

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

- **Appropriate law enforcement organization; and,**
- **Port administration (as applicable).**

4. Security plan amendments

All regulated stakeholders shall review their security plans and security related documents, and make formal amendments, as applicable, to reflect these mandatory reporting changes for continued compliance with the MTSR and the DFSR. Stakeholder shall submit all amendments to security plans directly to their TC Regional Marine Security Office for approval.

GUIDANCE:

Any event that meets the definition of a security threat, breach or incident, in accordance with either the MTSR or DFSR, must be reported as soon as possible after it occurs to the National TCSC.

It is recognized that immediate actions may need to be taken by stakeholders to initiate a response to a threat, breach or incident. In these cases, stakeholders must contact the National TCSC to report the security threat, breach or incident at the earliest possible moment once immediate actions have been taken to preserve life, safety, and security.

For greater clarity, as soon as possible is further defined as the first possible moment after an event has occurred without undue delay. To ensure ongoing compliance with the Regulations, stakeholders shall not wait until the next business day to report a security threat, breach or incident.

To determine whether an event necessitates reporting to TC, consider whether:

- Any established security policy, safeguard, measure or procedure was circumvented, regardless of the nature of the event (intentional or accidental) and regardless if the security of a vessel, facility, port or installation was affected;

- The event did or had the potential to threaten or affect the integrity of the security posture of the port, facility, vessel, ferry or ferry facility or the integrity of assets and infrastructure;

- The threat/event could impact other vessels, facilities or ports;

- The event could impact national security or the general security and ongoing functioning of the marine transportation system and its infrastructure;

- The event requires liaison and coordination with the regulatory or security community;

- The event may require the attendance of a TC Marine Security Inspector (to observe or provide regulatory guidance);

- The event has triggered a need to implement alternate security arrangements; or

- The event has otherwise impacted the ability of a port, facility, vessel or ferry to fully implement its security plan.

A non exhaustive list of examples of threats, breaches and incidents is included in Annex A. **This list is meant as a guide only.** Any event that meets the definition of a security threat, breach or incident must be reported as soon as possible without undue delay.

If in doubt whether an event requires reporting, Stakeholders are strongly encouraged to contact the National TCSC to provide a report.

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

NLegault

Nicole Legault
Director
Marine Security Operations

February 28, 2014

Annex A

This is a non exhaustive list of security incidents, threats and breaches that <u>must be reported as soon as possible to Transport Canada.</u>

If in doubt, please report it.

Security incidents

- Any security incident (physical or cyber) that has affected the security of personnel, cargo, a vessel, marine or ferry facility, an interface between vessels or between a vessel and a marine or ferry facility or another vessel;
- 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 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 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);

- 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; and
- 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;
- 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 persons, 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 ferry 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.

Transport Canada Transports Canada

To Report Marine Threats, Breaches and Incidents

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 with a carbon copy to your TC regional marine security office.

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

- **Appropriate law enforcement organization; and,**
- **Port administration (as applicable).**

Definitions:

Security threat: Any suspicious act or circumstance.

Security breach: A violation of security regulations, measures, rules or procedures.

Security incident: An incident that has affected security.

When in doubt, report it.