Transport Canada　Transports Canada

MARINE SECURITY OPERATIONS BULLETIN

No: 2016- 002

SUSPICIOUS ACTIVITY REPORTING

PURPOSE:

This Marine Security Operations Bulletin (MSOB) supports MSOB 2014-001 *Clarification of Transport Canada (TC) Marine Security mandatory threat, breach and incident reporting requirements* and serves as guidance for the reporting of suspicious activities.

This MSOB applies to all stakeholders subject to the *Marine Transportation Security Act* (*MTSA*), the *Marine Transportation Security Regulations* (*MTSR*), the *Domestic Ferries Security Regulations* (*DFSR*), the *Security Measures Respecting Designated Tall Ship Events*, and the Security Measures Respecting Tall Ships and Marine Facilities that Interface with Tall ships.

ACTION:

Port administrations, marine facilities*, vessel and tall ship security officers, operators of vessels, facilities and industry stakeholders who are subject to the *MTSA*, hereafter referred to as regulated stakeholders, are encouraged to use this bulletin when evaluating and reporting suspicious activities.

***For the purposes of this document, occasional-use marine facilities will be referred to as a marine facilities unless otherwise stated.**

BACKGROUND:

The reporting of suspicious activity, security threats, security breaches and security incidents is important to protecting the marine transportation system from attacks, staying ahead of evolving threats, maintaining situational awareness, understanding risks and remaining responsive.

The mandatory reporting of security threats, breaches and incidents allows Transport Canada the opportunity to recognize, analyze and respond to potential threats and security events. This requirement also enables Transport Canada to assess the adequacy of vessel security plans, tall ship security plans, port security plans and marine facility security plans to prevent security incidents. For more information about mandatory threat, breach and incident reporting requirements, please refer to MSOB 2014-001 (https://www.tc.gc.ca/eng/marinesecurity/operations-bulletins-menu-69.htm).

Canada

Suspicious activities may not meet the threshold for mandatory reporting to Transport Canada as described in MSOB 2014-001, and often go unreported. These activities may or may not seem significant on their own from a security standpoint yet may have a possible connection to national security or may indicate pre-attack planning against assets, either human, physical or cyber. Stakeholders are encouraged to report suspicious activities to Transport Canada.

Transport Canada treats all reports of suspicious activities as sensitive security information. Transport Canada will share the information with Canadian law enforcement agencies and public safety partners on a need to know basis. Transport Canada with its partners will use the information to identify trends and patterns, to assist in making decisions when addressing potential threats that may be identified and to assist those responsible for the development of port, marine facility and vessel security assessments.

SUSPICIOUS ACTIVITY:

Suspicious activity: A suspicious activity can cover almost any activity that is out of the ordinary, if that activity gives rise to suspicion that an individual or group is attempting to hide something, avoid authorities, or it generally falls outside a normal pattern of behaviour. It is an observed behaviour that could indicate pre-operational planning related to terrorism or other criminal activity.

The following criteria describe Transport Canada's recommendations for reporting suspicious activity. No description could cover all possibilities and Transport Canada understands that best judgment will be used when making reports.

Examples of suspicious activity may include:

- Unusual behavioral patterns, such as:
    - Not responding to verbal interaction or unusually avoiding eye contact;
    - Walking slowly in a deliberate fashion towards a potential target;
    - Excessive loitering;
    - Inappropriately dressed (wearing excessive clothing as to conceal something, or looking out of place);
    - Individuals who display excessive sweating, mumbling to oneself or displaying an unusually calm or detached demeanour;
    - Drivers who attempt to abandon a vehicle or act nervously;
    - Vehicles parked or individuals who stay (if applicable) for extended periods while

vessels, trains, ferries, tall ships, trucks, or buses come and go;

  - Observing the same individual(s) returning multiple times to the same area;
  - Individuals who carry on long conversation on pay phones or cellular phones;
  - Excessive nervousness or "doomsday" talk;
  - Excessive questions;
  - Lack of photo identification;
  - Agitation or rage;
  - Picture and video taking in a location where it would not be a normal activity, especially if the person has been asked earlier not to take photos;
  - Unusual use of binoculars;
  - Note taking or drawing;
  - Taking measurements;
  - Attempting to access unauthorized areas or areas by a means or method not normally used or out of the ordinary;

- Individuals seeking information or questioning vessel or marine facility personnel about the vessel, the marine facility/ the infrastructure/ the personnel; this includes individuals probing employees in person, on or off site, over the phone or via the internet about particular structures, functions, procedures at the marine facility, screening equipment or its IT systems;

- Apparent testing or observation of emergency services/response, including security drills and exercises;

- Damaging, manipulating, or defacing part of a marine facility/infrastructure, or vessel with malicious intent;

- Attempts to obtain training in security concepts, or other, unusual requests for specialized training in vessel operation, cargo transport, or handling capabilities;

- Unauthorized divers, swimmers, or vessels, in close proximity to a marine infrastructure or vessel;

- Unauthorized/unlicensed individual or group attempting to obtain precursor chemicals/agents, dangerous goods or toxic chemicals;

- Numerous visitors arriving and leaving at unusual hours;
- Unsuccessful attempts to access IT systems (e.g., someone from the same source keeps locking out accounts trying to force passwords, an automated script keeps probing a web server causing response problems);
- Unauthorized use of, or presence of unmanned aerial vehicles (UAVs-commonly known as drones);
- Activities in or around an adjacent marine facility, infrastructure, or vessel that in the opinion of the operator, may have an impact or influence on the security of their operations;
- Possession of materials that are not related to the business operations;
- Attempted use of forged or stolen documentation or identification and cover stories to blend in or attempt entry into a marine facility, port or vessel;
- Unusual assessments of internal and external lay-outs of buildings or request for building schematics or other sensitive marine facility or vessel information;
- Unusual "walk ins" to assess infrastructure and/or ask questions of staff;
- Attempted breaches, including those that are seemingly innocuous;
- Small vessels interfacing with SOLAS or non-SOLAS vessels; and
- Small vessels loitering or operating in an unusual manner.

REPORTING PROCEDURES:

Suspicious activity reporting: Suspicious activity, whether physical or cyber, may be reported anytime to the Transport Canada Situation Centre (SITCEN) by telephone at 1-888-857-4003 (toll free within Canada/U.S.) or 1-613-995-9737 and follow up information may be emailed to Sitcen@tc.gc.ca .

Stakeholders should provide the following information:

- Name of organization/source information (name, telephone number, e-mail address);
- Date and time of the suspicious activity;
- Date and time of reporting (if applicable, when information is received from a secondary source);
- Location of suspicious activity (province, city, marine facility name and location on the facility where the incident occurred - or Vessel name and location- , Port Authority name, if applicable;
- Description of suspicious activity (describe persons, vehicles, vessels, actions, routes taken, any equipment observed, nature of conversation / languages spoken);
- Actions taken by the reporting stakeholder;
- Who else was informed; and
- Other relevant information.

OTHER CRITICAL INFRASTRUCTURE RESOURCES:

In addition to reporting suspicious activity to Transport Canada, regulated stakeholders may also report suspicious activities, to the Royal Canadian Mounted Police (RCMP), the local police force, and the Canadian Cyber Incident Response Centre (CCIRC).

Note that reporting to these organizations is also voluntary. Transport Canada is continuing to work with other departments to streamline reporting requirements.

ROYAL CANADIAN MOUNTED POLICE (RCMP) AND OTHER LAW ENFORCEMENT

The RCMP has developed a suspicious incident reporting (SIR) system for critical infrastructure operators. The SIR was launched to collect information on suspicious incidents that may be related to national security. This system is designed to receive and capture data on suspicious incidents which meet two criteria:

- That have occurred at, or affect, Canadian critical infrastructure assets;
- They may have a possible connection to national security, meaning they may be indicative of either a physical or cyber pre-attack planning against one or more of Canada's critical infrastructure assets.

In addition to contacting Transport Canada, stakeholders are also strongly encouraged to report suspicious occurrences that meet these criteria to their local police service or to call the:

National Security Information Network at 1-800-420-5805 or by email at NSIN_RISN@rcmp-grc.gc.ca

For more information on the SIR, you are invited to email the RCMP's National Security Program SIR project at SIR-SIS@rcmp-grc.gc.ca.

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

CCIRC is Canada's national cyber security incident response team. CCIRC operates 24/7, with staff onsite 15/7 and on call for 9/7, and serves critical infrastructure organizations in Canada.

CCIRC's role is to assist infrastructure organizations in Canada to protect their cyber systems from compromise. They offer assistance in preventing, mitigating, and detecting malicious cyber activity to stakeholders free of charge.

CCIRC also serves as the single point of contact for owners and operators of critical infrastructure to report cyber incident to the Government of Canada and has a mandate to coordinate the national response to significant cyber incidents.

Critical infrastructure organizations who notice unusual activity on their systems, discover a malware infection or are the targets of other kinds of cyber incidents can report these incidents to CCIRC, 24 hours a day and free of charge. Information shared with CCIRC is anonymized before it is shared with other partners and is only shared with the permission of the affected organization(s).

To report a cyber- incident or subscribe to distribution lists to receive threat information and awareness products contact cyber-incident@ps-sp.gc.ca.

PORT SECURITY COMMITTEE:

The MTSR requires marine facility operators to participate in their local Port Security Committee. Transport Canada also encourages vessels and tall ships to participate in Port Security Committees. These committees are the best place to collaborate with partners at the port level for security and information sharing, including the resources, services and capabilities of other federal, provincial, territorial, local and private sector partners. To learn more about Port Security Committees contact your local port administration or your nearest Transport Canada Marine Safety and Security office.

QUESTIONS:

Transport Canada encourages stakeholders to report suspicious activities. If in doubt whether an event requires reporting, stakeholders are strongly encouraged to contact the National Transport Canada Situation Centre to provide a report.

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

Malick Sidibé
Director
Marine Security Operations

September 14, 2016

Reporting Suspicious Activity to Transport Canada

Suspicious activity, whether physical or cyber, may be reported anytime to the Transport Canada Situation Centre (SITCEN) by telephone at 1-888-857-4003 (toll free within Canada/U.S.) or 1-613-995-9737 and follow up information may be emailed to Sitcen@tc.gc.ca