CIRCULAR NO.6-2022/MARITIME SECURITY

20 SEPTEMBER 2022

These Circular serves to provide regular information from the Maritime Security Committee established by law about maritime security and security information of interest in Solomon Islands.

The International Convention for the Safety of Life at Sea (SOLAS) 1974 have force of law in Solomon Islands as per the Shipping Act 1998 as amended. The Chapter XI-2 of SOLAS on Special Measures to Enhance Maritime Security and the International Ship and Port Facility Security (ISPS) Code contain detailed security-related requirements for governments, port authorities and shipping companies visited by, or operating vessels engaged in international voyages. The Maritime Safety Administration (Ship and Port Security) Regulations 2011 provide for maritime security management and responsibilities in Solomon Islands.

SECURITY LEVEL

Solomon Islands is currently at the **Security Level 1**. Section 2.1 of the ISPS Code Part A defines **Security Level 1** as: "*the level for which minimum appropriate protective security measures shall be maintained at all times.*"

Security Level 2 *"means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident."*

Security Level 3 *"means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target."*

FROM THE MARITIME SECURITY COMMITTEE

At its last meeting, the Maritime Security Committee (MSC) discussed an emerging issue related to the operations of vessels usually engaged solely in domestic trade and from time-to-time in international voyages for example to dry-dock or respond to a one-off shipment. This includes some registered vessels servicing Nauru for the construction of the international port there.

The Committee agreed that exemption to security measures on board ships engaged exceptionally in international voyages should not be considered anymore given the international security environment and threats. No country and no vessel is exempt from security threats. Any vessels engaged in an international voyage should implement security measures and those of 500 gross tonnage and more comply to the Chapter XI-2 of SOLAS Convention and the ISPS Code.

SIMA informed the Committee that there is now a process to certify security measures on board vessels registered in Solomon Islands and engaged in international voyages even though in exceptional circumstances. All domestic ship owners are encouraged to consider security before engaging their vessel in an international voyage. This will also better prepare Solomon Islands ship operators to seize any opportunity of regional cabotage (Papua New Guinea, Vanuatu, Australia).

DID YOU KNOW?

WHAT ARE THE IMPLICATIONS OF SECTION 21. OF THE SHIP AND PORT SECURITY REGULATIONS 2011

It is about **Ship Security**! Any shipping company which owns a ship engaged in international voyage and subject to the 2011 regulations must:

(a) appoint a **Company Security Officer (CSO)** to oversee all company's security arrangements;
(b) appoint a **Ship Security Officer (SSO)** onboard each of its vessels responsible for security onboard;
(c) ensure a **Ship Security Assessment (SSA)** is conducted and a **Ship Security Plan (SSPs)** is developed; and
(d) have **SSA-SSP approved,** and an **audit conducted by SIMA** for issuance of the **International Ship Security Certificate**.

NEWS

WHAT IS SHIP SECURITY ALERT SYSTEM?

The Ship Security Alert System (SSAS) is a safety measure for strengthening ship's security and subduing acts of piracy and/or terrorism against shipping. Widely Acknowledged as a part of the International Ship and Port Facility Security Code (ISPS code), the SSAS complements the International Maritime Organization (IMO)'s attempts to increase maritime vessel security.

COSPAS-SARSAT, with IMO's cooperation, came up with this project of SSAS. The basic idea is that in case of an attempted piracy effort, terrorist act, or any other incident which can be defined as a threat to the ship under the maritime security, the ship's SSAS beacon would be activated, responding to which an appropriate law-enforcement or military forces would be dispatched for rescue. The SSAS beacon and the Aircraft Transponder Emergency Code 7700 are operated on the fundament of similar principles.

Source: https://www.marineinsight.com/marine-piracy-marine/what-is-ship-security-alert-system-ssas/

PRODUCT ALERT – WHAT IS PHISHING?

Phishing is a social engineering cybersecurity attack which occurs when cybercriminals impersonate a trusted sender to deceive victims into sharing sensitive information by clicking malicious links or attachments. It can also give cybercriminals the opportunity to install malware on the devices of victims.

Phishing attacks can directly undermine Pacific national security by compromising access to systems and sensitive information. Access our primer to learn more about phishing and ways to reduce the impact of this threat.

Source: http://www.pacificfusioncentre.org/

CYBER SECURITY AND THE INTERNATIONAL MARITIME ORGANIZATION

Towards the safe and secure operation of vessels at sea and ashore, the International Maritime Organization (IMO) recently added cyber security requirements to critical safety management systems (SMS) under IMO Resolution MSC.428(98). In recognition of the urgent cyber threats to the global shipping industry and understanding the massive global impact that a high-profile incident in a highly trafficked area, like the Suez Canal, can have on the world economy and geo-political environment, these regulations are long overdue. As of January 1, 2021, operators must urgently address cyber security risks in order to maintain compliance ahead of the annual verification of their Document of Compliance (DOC).

The IMO resolution effectively addresses maritime cyber security risks inherent in safety management systems within the International Safety Management (ISM) Code. A key element of effective cyber risk management is a process to harden SMS components and segment and secure portions of the network on which they operate. As a major cyber incident attack vector, unpatched operating systems and other critical software must be effectively and routinely updated to maintain regulatory compliance with the ISM Code. Key risk assessment management processes must include the timely and routine patching and updating of onboard SMS components and other software infrastructure.

Source: Compliance with the IMO 2021 Cyber Security Regulation | Resilio Blog

CONTACT

For anything related to maritime security please contact Ms. Duri Qalorusa, Senior Officer, Maritime Security at SIMA duri.qalorusa@sima.gov.sb.