Republic of the Marshall Islands

MARITIME ADMINISTRATOR

11495 COMMERCE PARK DRIVE, RESTON, VIRGINIA 20191-1506
TELEPHONE: +1-703-620-4880 FAX: +1-703-476-8522
EMAIL: shipsecurity@register-iri.com WEBSITE: www.register-iri.com

SHIP SECURITY ADVISORY NO. 13-20

To: **Owners/Operators, Masters, Company Security Officers, Recognized Security Organizations**

Subject: **CYBER RISK MANAGEMENT – REVISED INDUSTRY GUIDELINES AND UNITED STATES PORT STATE CONTROL MEASURES**

Date: **30 December 2020**

The Republic of the Marshall Islands (RMI) Maritime Administrator hereby draws attention to the following updates regarding the upcoming maritime cyber risk management requirement:

Industry Cyber Guidelines (Version 4)

The fourth edition of the industry cyber risk management guidelines, *Guidelines on Cyber Security Onboard Ships (Version 4)*, is now available and lays the foundation for further improvements and refinement of companies' cyber security risk assessments.

The latest update to the cyber guidelines is published at a time when shipowners and ship managers must implement cyber risk management throughout the safety management systems (SMS) by the time of a vessel's first Document of Compliance audit **after 1 January 2021**. While the previous version (version 3, dated November 2018) offered the necessary guidance for the initial work of implementing cyber risk management in the SMS, the new version contains several improvements.

The fourth version contains general updates to best practices and features improved guidance on the concept of risk and risk management. The improved risk model now defines 'threat' as "the product of capability, opportunity, and intent;" and explains the 'likelihood' of a cyber incident as "the product of vulnerability and threat." While few safety-related cyber incidents have been reported in the maritime industry thus far, this improved risk model explains why this must not cause shipping companies to lower their guard.

United States Coast Guard (USCG) Port State Control

The USCG Office of Commercial Vessel Compliance has published Work Instruction CVC-WI-027, *Vessel Cyber Risk Management*.

This SSA is evaluated annually by the Administrator and expires one year after its issuance or renewal unless otherwise noted, superseded, or revoked.

This Work Instruction provides guidance to USCG Marine Inspectors and Port State Control Officers for assessing cyber hygiene onboard applicable vessels, as well as compliance options if deficiencies are observed. **Please note that nonconformities related to cyber risk may result in a Code 30 detainable deficiency at United States ports.** CVC-WI-027 and other Work Instructions are available at the USCG Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) website.

For additional information and a list of maritime cyber risk management resources (SS-200), please refer to RMI Marine Guideline 2-11-16, *Maritime Cyber Risk Management* or contact shipsecurity@register-iri.com.