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: marsec@register-iri.com WEBSITE: www.register-iri.com

SHIP SECURITY ADVISORY NO. 08-26

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

Subject: **MARITIME CYBER SECURITY: TARGETING OF SHIPBOARD NETWORK INFRASTRUCTURE**

Date: **30 October 2026**

The Republic of the Marshall Islands (RMI) Maritime Administrator (the "Administrator") draws attention to the targeting of commercial vessels by hostile cyber actors. Internet-facing network infrastructure on board is being used as an attack vector into vessel information technology (IT) and operational technology (OT) systems.

1.0 Issue

1.1 This Advisory is prompted by confirmed law enforcement and port State action against commercial vessels bound for the United States (US) during August 2026, and by notifications received by owners and operators from foreign law enforcement and computer security incident response authorities during the same period.

2.0 Background

2.1 The US Coast Guard (USCG) and the Federal Bureau of Investigation (FBI) have confirmed that two vessels bound for the US were subjected to suspected cyber attacks during August 2026. One was boarded on 21 August 2026 in the Gulf of Mexico by a team of USCG law enforcement, vessel inspection and cyber protection personnel, and an FBI cyber team, following indications that the vessel's network had been compromised by foreign cyber actors. A second vessel was boarded on 24 August 2026.[1]

2.2 The first vessel is reported to have been in the Strait of Gibraltar at the time of compromise and to have lost communications for a period in excess of 30 hours. The agencies reported no resulting operational disruption, vessel instability, physical danger to crews, or environmental impact.

[1] ABC News, Coast Guard, FBI investigating after 2 oil tankers bound for US hit with cyberattacks: Sources, 16 September 2026; and CBS News, Coast Guard, FBI boarded Texas-bound commercial oil tanker to investigate cyberattack, 15 September 2026.

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is evaluated annually by the Administrator and expires one year after its issuance or renewal unless otherwise noted, superseded, or revoked.

2.3 Separately, and not derived from public reporting, notifications that originated with a national police authority were relayed through a national computer security incident response team to the charterer and, in turn, to the vessel operator. One such notification identified the vessel by name and International Maritime Organization (IMO) number, stated that the vessel is compromised, and identified a firewall appliance installed on board by its public internet protocol address, requesting preservation of the logs held on that device. Notifications of this character may reach a Company by a commercial route rather than from a maritime authority and may arrive before any port State contact.

2.4 No State or group has claimed responsibility and no government has made a public attribution.

3.0 Assessment

3.1 Commercial vessels may be the subject of deliberate network targeting rather than opportunistic infection. The pattern of notification, involving national police and national incident response authorities identifying named vessels and named devices, is consistent with intelligence-derived reporting rather than with routine antivirus detection on board.

3.2 Internet-facing network infrastructure at the satellite communications boundary, principally firewalls, routers, and virtual private network (VPN) concentrators, is the most likely point of entry. These devices are reachable from the internet by design, frequently administered remotely by a third party, often several firmware versions behind, and not covered by the antivirus software installed on shipboard workstations. The USCG and the FBI have separately identified Fortinet FortiGate devices in use by vessels and facilities in the US Marine Transportation System (MTS) as the subject of exploitation by nation-state threat actors and have advised that the credential-compromise campaign known as FortiBleed has exposed administrator credentials for internet-facing FortiGate firewalls and secure socket layer (SSL) VPN gateways at scale. See USCG and FBI Maritime Cyber Alert 02-26, *Fortinet FortiGate Vulnerabilities*, and FBI and United States Secret Service advisory JCSA-20261006-01.

3.3 Detection has occurred well after compromise and by parties external to the vessel. Absence of observed anomalies on board should not be treated as evidence that no compromise has occurred.

3.4 Compromise at the communications boundary places an actor in a position to observe voyage, cargo, and crew information, interfere with shore communications, and, where networks are not segregated, reach systems supporting navigation and cargo operations. The risk at present falls on information, the availability of communications, and commercial and port State standing, with the potential for consequences to safety where IT and OT networks are not separated.

3.5 Exposure is not confined to equipment on board. The US Maritime Administration (MARAD) has advised that foreign-manufactured port equipment and logistics data platforms may create vulnerabilities in maritime IT and OT systems, and that third-party network traffic should be treated as untrusted until validated. Vessels that exchange data with port and terminal systems, or that grant shore-based parties access to shipboard networks during port calls, may be exposed through those connections. See MARAD Maritime Security Communications with Industry (MSCI) Advisory 2026-014.

4.0 Recommended Action

4.1 The measures addressing this threat are already set out in existing guidance and are not restated here. Companies should manage cyber risk in the safety management system under RMI Marine Notice (MN) 2-011-13 and in the ship security plan under MN 2-011-16, applying RMI Marine Guideline (MG) 2-11-16, IMO Circular MSC-FAL.1/Circ.3/Rev.4, and *The Guidelines on Cyber Security Onboard Ships*. Supporting resources are listed in the *Maritime Cyber Risk Management Resources* (MARSEC-200).[2]

4.2 In light of the incidents described above, and based on the measures listed in §4.1 above, Companies are reminded to ensure that:

.1 administrative interfaces of firewalls, routers, satellite terminals, and VPN concentrators are not reachable from the internet, and that any necessary remote administration is restricted to named addresses and protected by multi-factor authentication;

.2 firmware on those devices is at a current supported release, and that any device beyond end of support is replaced rather than left at the network boundary. See the Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive 26-02;[3]

.3 default, dormant, shared, and departed-personnel accounts have been removed, and that unused services, VPN portals, and remote management protocols are disabled;

.4 every party holding remote access to shipboard systems is identified, that access is granted for a defined purpose and period, supervised and logged, and that standing unsupervised access is withdrawn. See also MSCI Advisory 2026-014;

---

[2] IMO Circular MSC-FAL.1/Circ.3/Rev.4 was issued on 28 May 2026, following approval by the Facilitation Committee at its 50th session and the Maritime Safety Committee at its 111th session, and supersedes Rev.3 of 4 April 2025.

[3] Binding Operational Directive 26-02, Mitigating Risk From End-of-Support Edge Devices, was issued on 5 February 2026. See also the joint CISA, FBI and United Kingdom National Cyber Security Centre fact sheet, Reducing the Attack Surface for End-of-Support Edge Devices.

.5 logging is enabled on network appliances and forwarded off the vessel or exported on a schedule, since these devices hold logs in limited local storage that overwrites as new events are recorded; and

.6 IT and OT networks are separated, and that crew welfare access has no route to navigation, cargo control, ballast, or machinery systems.

4.3 Where Fortinet FortiGate devices or SSL VPN gateways are installed, the mitigations set out in Maritime Cyber Alert 02-26 and in JCSA-20261006-01 should be applied. Companies should note that credentials exposed through FortiBleed remain valid after a firmware upgrade, so patching alone does not close the exposure.

4.4 Shipboard personnel should report to the Company Security Officer (CSO), without delay, any unexplained loss or degradation of satellite communications, any unexpected reboot, configuration change or administrator logon on network equipment, any behavior of Electronic Chart Display and Information Systems, Global Navigation Satellite Systems, Automatic Identification Systems, or radar inconsistent with independent position fixing, and any contact from an external party suggesting that the vessel or the Company has been compromised.

5.0 Response to a Suspected Compromise

5.1 After reviewing lessons learned from an investigation of a recent incident, the Administrator recommends the following actions be considered when a compromise is suspected. These actions to be considered are supplemental to the incident response measures set out in USCG and FBI Maritime Cyber Alert 02-26 and in FBI and US Secret Service advisory JCSA-20261006-01:

.1 notify the CSO, the Company, and the Administrator without delay, and notify the port State where the vessel is in or approaching its waters;

.2 preserve evidence in place. Do not reimage, reset, reconfigure, upgrade firmware, restore from backup, or power down an affected system or network appliance until the scope is understood;

.3 export and preserve the logs and configuration of any identified device immediately, together with its account list and remote access configuration, before local storage overwrites them, and secure Voyage Data Recorder data covering the period concerned;

.4 recognize that antivirus scanning of workstations neither examines nor preserves anything held on a network appliance, and that scanning alters file access times and may quarantine or delete the artifacts an examination would rely upon. Where scanning has been carried out, preserve the quarantine store and scan logs and record what was run, when, and with what result;

.5 record all actions taken, with times, from the first indication; and

.6 engage the Company's protection and indemnity association and where navigation, machinery, or cargo systems may be affected, the Recognized Organization, at an early stage.

5.2 Where a port State or foreign authority proposes to examine shipboard systems, the Administrator asks to be informed in advance and to be provided with any instrument governing access to the vessel's systems or data before it is executed. Such an instrument may make factual certifications and accept risk on behalf of the owner and should not be executed by the master alone without the Company's express written instruction.

6.0 Port State Considerations

6.1 The USCG final rule, Cybersecurity in the Marine Transportation System, 90 FR 6298, took effect on 16 July 2025 and is codified at 33 CFR, Part 101, Subpart F. It applies to US-flagged vessels and to regulated facilities and does not apply directly to RMI-flagged vessels. The USCG has nevertheless indicated that port State control scrutiny of indicators of poor cyber risk management on foreign-flagged vessels will increase, examined through International Safety Management (ISM) Code and International Ship and Port Facility Security (ISPS) Code compliance.[4]

6.2 A Captain of the Port order may be issued without a written statement of the concern that prompted it and without stated criteria for its release. Where an order is issued, the Company should request in writing a statement of the basis for the order and of the conditions that must be satisfied for it to be rescinded and should provide a copy of the order to the Administrator.

7.0 Incident Reporting

7.1 Companies are reminded that all maritime cyber incidents involving RMI-flagged vessels are to be reported to the Administrator by submitting a *Report of Maritime Cyber Incident* (MI-109-5) under MG 2-11-16. Data received is held in confidence and reported incidents are not attributed to any vessel or Company. Security incident reporting obligations under MN 2-011-16 also apply.

7.2 Where an external party notifies the Company that a vessel has been compromised, the notification itself, and any device, address, or indicator it identifies, should be provided to the Administrator when it is received and not withheld pending the outcome of an investigation.

[4] Cybersecurity in the Marine Transportation System, final rule, 90 FR 6298, published 17 January 2025, docket USCG-2022-0802, effective 16 July 2025, codified at 33 CFR 101.600 et seq.

7.3 Reports and notifications may be made at any hour to marsec@register-iri.com, dutyofficer@register-iri.com, or +1 571 441 1885.

7.4 Vessels in or bound for US waters that identify a cyber incident should additionally report to the USCG at maritimecyber@uscg.mil, to the Coast Guard Cyber Command 24-hour watch at +1 202 372 2904, and to the National Response Center at +1 800 424 8802. Reporting only to a port State does not satisfy the requirements on reporting to the Administrator referenced in § 7.1 above. Further US Government reporting contacts are listed in MSCI Advisory 2026-014.

8.0 References

.1 MN 2-011-16, *International Ship and Port Facility Security (ISPS) Code*

.2 MN 2-011-13, *International Safety Management (ISM) Code*

.3 MG 2-11-16, *Maritime Cyber Risk Management*

.4 *Maritime Cyber Risk Management Resources* (MARSEC-200)

.5 *Global Maritime Security Contacts* (MARSEC-210)

.6 IMO Circular MSC-FAL.1/Circ.3/Rev.4, *Guidelines on Maritime Cyber Risk Management*

.7 Shipping industry associations, *The Guidelines on Cyber Security Onboard Ships, version 5*

.8 USCG, Cybersecurity in the Marine Transportation System, 90 FR 6298

.9 33 CFR, Part 101, Subpart F, *Cybersecurity*

.10 US Maritime Administration, *Maritime Security Communications with Industry advisories*

.11 CISA Binding Operational Directive 26-02, *Mitigating Risk From End-of-Support Edge Devices*

.12 USCG and FBI, Maritime Cyber Alert 02-26, *Fortinet FortiGate Vulnerabilities*

.13 FBI and United States Secret Service, JCSA-20261006-01, *FortiBleed Operations Continue Targeting Exposed Systems Leading to Reports of Lockouts*

.14 MARAD, MSCI Advisory 2026-014, *Worldwide-Foreign Adversarial Technological, Physical, and Cyber Influence*