

GUIDANCE NOTE 03/2025 (Rev1.0)

APPROVING AMENDMENTS TO SHIP SECURITY PLANS

To: Owners, Managers, Company Security Officers, Masters and Ship Security Officers

1. BACKGROUND

- 1.1 The purpose of this Guidance Note is to clarify which amendments to an approved Ship Security Plan (SSP) require approval from the Cayman Islands Shipping Registry (CISR) before being implemented on board a Cayman Islands ship.
- 1.2 This Guidance Note should be read in conjunction with [Shipping Notice 08/2005](#) (*Minimum Requirements for Ship Security Assessments (SSA) and Ship Security Plans (SSP)*).
- 1.3 This Guidance Note has been revised to clarify that Recognized Security Organizations (RSO) may approve amendments to an approved SSP if that RSO also issued the International Ship Security Certificate (ISSC) for the ship.
- 1.4 This Guidance Note replaces Shipping Notice CISN 01/2020.

2. SSP APPROVAL

- 2.1 Ship Security Plans (and the Ship Security Assessment (SSA) on which they are based) must be submitted to CISR before the Interim Verification required by ISPS A19.4.2 can be carried out.
- 2.2 The Ship Security Plan must be approved by CISR before the Initial Verification required by ISPS A19.1.1.1 can be carried out.
- 2.3 A RSO may not conduct the initial approval of an SSP.
- 2.4 Ships Security Plans and amendments requiring approval by CISR should be submitted to technical@cishipping.com.

3. AMENDMENTS TO SSPs THAT REQUIRE APPROVAL BY CISR OR THE RECOGNIZED SECURITY ORGANIZATION ISSUING THE ISSC

- 3.1 ISPS A9.5 requires that an Administration shall determine which changes to an approved SSP or any security equipment specified in an approved SSP shall not be implemented unless the relevant amendments are approved by the Administration.
- 3.2 The Annex to this Guidance Note lists the amendments that are required to be approved before being implemented on board a Cayman Islands ship.
- 3.3 A RSO may approve the amendments listed in the Annex if that RSO also issued the ISSC for that ship.
- 3.4 Other amendments to the SSP may be implemented without prior approval from CISR. These amendments will be reviewed as part of the next ISPS verification carried out on board the ship.

4 CHANGES IN COMPANY SECURITY OFFICER (CSO) IDENTITY AND CONTACT DETAILS

- 4.1 For a change in CSO a new [Company Contact Details](#) form should be submitted, along with documentary evidence that the person's qualifications and experience meets the requirements of IMO MSC/Circ.1154, to technical@cishipping.com.

Annex

- 1 *Method of acknowledging changes in security levels.*
- 2 *Responses at security level 3 including:*
 - *security measures that could be taken, in close co-operation with those responding to an incident at a port facility, in response to security instructions from Governments; or*
 - *liaison to ensure close co-operation with those responding to the incident, and the port facility.*
- 3 *Procedures for controlling access to the ship including:*
 - *restricted areas including changes in location, boundaries, times of application and access protocols;*
 - *supervising cargo handling, delivery of ship stores, handling unaccompanied baggage;*
 - *monitoring the security of the ship including increased frequency and details of security patrols; or*
 - *auditing, reviewing and updating the SSP.*
- 4 *Procedures for reporting incidents to the company, CISR, coastal states when at sea, or ports.*
- 5 *Frequency for testing, calibration, and maintenance procedures for security equipment.*
- 6 *Procedures for maintaining confidentiality of SSP, SSA and records.*
- 7 *Frequency of training including security drills, exercises and providing security briefings to ship's personnel.*
- 8 *Changes to the SSAS including activation points, type of system or process related to receiving alerts in the Company.*