Inspections and Surveys - ISPS (2026)

SECURITY DRILL AND COMPREHENSIVE EXERCISE

The Member State / flag State shall ensure (monitor/supervise) that security drills and more comprehensive exercises are conducted on board ships, since Regulation (EC) No 725/2004 makes the requirements of the ISPS Code mandatory for ships falling within its scope, and Member States monitor compliance both as flag States and as port States. In addition, Member States/flag States should ensure this through monitoring, inspections, or reviews that the distinction between security drills and exercises, as well as their purposes, is understood and implemented correctly.

Security drills and exercises are mandatory requirements applicable to ships in accordance with the ISPS Code (as it becomes applicable through Regulation (EC) 725/2004).

Ships shall carry out:

Security drills at least once every three months (and, in addition, an extra drill within one week if more than 25% of the crew is replaced and the change includes persons who have not participated in a drill during the previous three months).

An exercise at least once in each calendar year, so that the interval between exercises does not exceed 18 months.

Security Drill / Operational Drill

Purpose: to ensure that the ship's personnel are proficient in their own security duties and that the procedures of the Ship Security Plan (SSP) work in practice.

Nature: operational, practical performance - a single procedure, task or routine is practised and tested (not the whole system).

Form: a smaller, crew-oriented and practically focused drill in which a specific procedure, task or routine is tested and practised (e.g. control measures, baggage inspection, use of security equipment). In addition, a security drill shall test individual parts/elements of the Ship Security Plan (e.g. certain threat scenarios).

More Comprehensive Exercise / System Exercise

Purpose: to test a broader part of the security system/arrangements: communication, coordination, access to resources and response.

Nature: more extensive than a security drill; often other actors also participate (e.g. the Company Security Officer (CSO), the Company Chief Information Security Officer (CISO), the Port Facility Security Officer (PFSO), authorities, sometimes also other ships/organizations).

Form: may be a practical (full-scale) exercise, a tabletop exercise (seminar/simulation exercise) or combined with other exercises (e.g. SAR or various emergency exercises including cyber/hybrid dimensions such as organized crime).

MINIMUM CONTENT OF AN ISPS EXERCISE REPORT UNDER EU REQUIREMENTS

Use these as minimum requirements when documenting each ISPS drill/exercise conducted on board:

Ship identification details
- ship's name
- IMO number

Exercise identification details
- date
- start and end time
- ship's position / port / terminal
- security level
- type of drill or scenario

Basis / reason for the exercise
- scheduled quarterly drill, more comprehensive exercise (annual) or
- drill after crew change (>25%), or
- drill related to a specific elevated security threat (incl. cyber/hybrid dimensions such as organized crime).

Objectives
- which subsection of the Ship Security Plan (SSP) was tested

Examples: access control, protection of restricted areas, search procedures, response to a suspicious package, unauthorized boarding, communication, cyber incident, actions by the Ship Security Officer (SSO). Alternatively, a preparedness exercise, including cyber/hybrid dimensions such as organized crime.

Scenario summary
- brief description of the drill / simulated event.

Participants
- the master, the Ship Security Officer (SSO), watchkeeping personnel / other personnel and search team
- possible participation from shore side (the Company Security Officer (CSO), Company Chief Information Security Officer (CISO), the Port Facility Security Officer (PFSO), authorities (incl. cyber security center) if they have participated).

Measures taken
- Measures taken by the crew/participants, step by step
- communication carried out (internal/external)
- access control (incl. digital access) or search measures
- any alarm / notification / reporting stages tested.

Equipment / systems tested
- radios / telephones / internal communication (PA)

- computer systems
- access control arrangements
- lighting / CCTV / locks / security barriers, where applicable
- other security equipment used in the drill.

Results / evaluation
- whether the objectives of the drill were achieved
- observed deficiencies
- feedback from crewmembers who participated in the drill
- feedback from competent authority/authorities, if they participated in the drill
- delays, misunderstandings, equipment failures or shortcomings in the Ship Security Plan (SSP).

Corrective actions
- what is to be corrected
- who is responsible
- target date / completion date

Debriefing note
- time of the debriefing
- persons participating
- key lessons learned

Approval / signature
- signature of the Ship Security Officer (SSO)
- approval by the master, if the company's procedure so requires
- distribution / filing location (security folder and/or electronic system)
- entry in the ship's logbook.

DOCUMENT REVIEW BY THE COMPETENT AUTHORITY

The Finnish Transport and Communications Agency Traficom can, by reviewing ships' annual security drill and exercise plans as well as reports on security drills and exercises, ensure that the security drills, exercises and reporting (documentation) comply with the requirements of Regulation (EC) No 725/2004 of the European Parliament and of the Council (including Annexes).