Guidance Paper on Requirements for the Audit and Review of Security Plans

Purpose

The purpose of this guidance paper is to assist Maritime Industry Participants (MIPs) who are required to have a security plan, to meet their obligations with respect to the audit and review requirements in the Maritime Transport and Offshore Facilities Security Regulations 2003 (the Regulations).

Background

Guidance issued by the Department in 2010 to MIPs was intended to provide an example to MIPs on audit and review requirements, yet it resulted in this example being assumed by some regulated MIPs as mandatory. This new guidance is intended to ensure that regulated MIPs understand they have complete discretion as to scheduling audits and reviews. The schedule should reflect the individual circumstances of the regulated MIP. The audit is a tool to assist a regulated MIP to implement their security plan.

Regulatory Requirments

For a maritime, ship or offshore security plan to be approved the Secretary (or delegate) must be satisfied that it addresses all the requirements listed in the *Maritime Transport and Offshore Facilities Security Act 2003* (the Act) in regards to the form and content of the plan (Maritime ss47-49, Ship ss66-68, Offshore ss100G-I). These requirements, listed in the Act, include any matters prescribed in the Regulations (Maritime s47, Ship s66, Offshore s100G). One of the matters prescribed in the Regulations is the auditing and reviewing of security plans (regs 1.50, 3.10, 4.105 and 5A.10).

The Regulations require a security plan to include:

- a schedule of security plan audits by internal and external auditors; and
- the procedures for conducting a security plan audit, including the process for selecting auditors who are independent of the matters being audited (Maritime reg 3.10, Ship reg 4.105, Offshore reg 5A.10).

The Regulations require a security plan to include the:

- circumstances in which a review will occur, aside from a maritime transport security incident; and
- procedures for conducting a review, including the consultation process (Maritime reg 3.10, Ship reg 4.105, Offshore reg 5A.10).

Once a security plan has been approved there are additional requirements in regards to audits and reviews of security plan.

- a regulated MIP must comply with the approved security plan and conduct audits and reviews in accordance with the procedures in the approved security plan (reg 1.50).

- the records of an audit or review must be kept for seven years (reg 1.50); and
- a regulated Australian ship must keep a record of audits and reviews in relation to the ship and which must be available for inspection in accordance with the Act (reg 1.55(1)(n)).

These requirements are consistent with Australia's international obligations under the

Safety of Life at Sea Convention and the *International Ship and Port Facility Security Code* (ISPS Code).

Compliance

The regulatory requirements will need to be set out in the regulated MIPs' security plan.

Once the security plan has been approved the schedule must be adhered to. However, a regulated MIP may choose to submit a variation to their security plan to change the schedule of audits.

Audits

Auditing is the inspection or examination of measures, procedures and activities contained within an approved security plan to determine if they have been implemented correctly.

The Regulations provide a definition of a security plan audit at reg 1.03.

Under the current legislation the minimum requirement is one internal and one external audit during the life of the security plan.

The audit schedule and procedures included in security plans should be robust enough to provide the regulated MIP with an understanding of whether the security plan in its current form is being appropriately implemented.

Regulated MIPs should consider:

- the outcome of their security assessment;
- the size and complexity of their activities;
- the maturity of their organisation; and
- whether any significant changes to operations are planned during the life of the plan when developing an audit schedule.

Example:

A schedule of audits can be in a variety of formats including:

- Date based: December 2016 and June 2018.
- Time span: within two years of the approval of the security plan and again prior to expiration of the security plan.
- Frequency: every 18 months from the approval of the security plan.

Internal and external audits

There is no definition in the Act or the Regulations of an internal or external audit or auditor. The ISPS Code defines an auditor as a person or entity separate from the activities being audited, this is consistent with the ordinary meaning of an auditor. This means that a person conducting an internal audit of the security activities specified in a security plan must be someone who is not responsible for the development or

implementation of the security plan. An external auditor is to be independent not only of the matters being audited but also from the regulated MIP.

Example

A regulated MIP engages an external auditor to conduct an audit of a range of regulatory requirements including maritime security; maritime safety and workplace health and safety.

Example

A regulated MIP may enter into a reciprocal agreement with other regulated MIPs to undertake external audits of each other's approved security plans. This could provide value networking and personal development opportunities for staff.

An auditor shall be considered external even where both the auditor and the regulated MIP are part of the same multinational corporation, as long as they are from separate legal entities.

Example

The regulated MIP is Company AA (Australia) and the external auditor is from Company AA (United Kingdom). While the two companies may take their management and strategic direction from the parent or holding company that in no way diminishes the separate and independent legal status of each company.

An audit which is undertaken by the Department does not constitute an external audit.

It is the responsibility of the Security Officer to ensure internal and external audits occur in accordance with the requirements of their security plan and are conducted by persons who are independent of the matters being audited. Persons are not considered independent of the matters being audited if they provide services required by a security plan to the industry participant being audited.

Example

An auditor who also provides contracted services required under the security plan to the industry participant being audited is not considered independent.

Reviews

A review is an assessment and evaluation of an approved security plan as a whole (including its procedures and measures) to ascertain if it is effective and adequate to meet the risks identified in the security assessment. The Regulations provide a definition of a security plan review at reg 1.03.

A review of a security plan is mandated after a maritime transport security incident to ensure the regulated MIP considers the adequacy of the security measures in the plan in the light of the incident (reg 1.50(2)). There is no set frequency for reviews of a security plan.

Example

Other circumstances where it could be beneficial for a regulated MIP to conduct a review are:

- if the security regulated entity is altered, for example, a port facility is modified;

- an audit of the regulated MIP identifies failings in the organisation or questions the continuing relevance of a significant element of the security plan;
- after the threat of a maritime transport security incident; and/or following changes in ownership or operational control of the security regulated entity.

A security plan must also include the procedures for conducting a security plan review, including a process for consultation during the review. Consultation is a requirement to ensure security measures and procedures are adequate and assists with the appropriate implementation of the security plan.

If an audit or review of a security plan identifies a failing, it is expected that the regulated MIP will undertake corrective action. In some cases, the regulated MIP may need to submit for approval a variance or revision of the security plan.