COMPLIANCE CODE FOR CLASS U4 PERMITS

Compliance Code history

Version	Date of Effect	Description
1	03/08/2017	Compliance Code first issue
2		
3		
4		
5		

Purpose

The purpose of this *Compliance Code* is to establish a standard set of requirements for the systems of *Nuclear Material* Control and *Nuclear Security* for all Class U4 Permits to Possess *Nuclear Material* issued under section 16 of *the Act*. It also sets out forms for the submission of applications, notifications and reports.

Scope

This *Compliance Code* applies to Permits identified under paragraph 3 of the Permit as a Class U4 permit. The requirements of the Code apply to all *nuclear material* in the possession of the Permit Holder except *nuclear material* which is declared under section 11 of *the Act* as exempt from the application of Part II of *the Act*.

Objective

The objectives of the systems for *nuclear material* accounting and control, and *nuclear security* are to:

- protect against unauthorised removal (theft) of *nuclear material* ;
- locate and recover missing *nuclear material*;
- protect *nuclear material* against sabotage;
- mitigate or minimize the radiological consequence of sabotage; and
- maintain control of *nuclear material*.

1. **Nuclear Material Accounting and Control (NMAC) System**

1.1. The Permit Holder shall:

1.1.1. maintain records details of each separate:

a) receipt of *nuclear material*, date of receipt, name and address of the consignor and of the carrier, if any; and

b) loading of *nuclear material*, including date of loading, name of ship, and name and tile of person accepting receipt of the material for the shipping line;

1.1.2. maintain organisational arrangements enabling the Permit Holder to determine the precise location of any material on the Permit Holder's inventory in less than 2 hours;

1.1.3. detect any *loss of control* of *nuclear material*; and

1.1.4. retain records of transfers of *nuclear material* for a period of 5 years.

1.2. The Permit Holder shall notify the *Director General* if the vessel does not have or is not required to have a Ship Security Plan.

2. **Arrangements for Storage Incidental to Transport**

In addition to stipulations under the International Maritime Organisation's International Ship and Port Facility Security (ISPS) Code and the *Maritime Transport and Offshore Facilities Security Act 2003* that requires Port Security Plans, Maritime Security Plans, the Ship Security Plan (SSP) and the International Maritime Dangerous Goods Code (IMDG) for Class 7 – Radioactive material, the Permit Holder shall maintain *nuclear material* specific arrangements for the incidental storage of *nuclear material*.

2.1. For Australian secure storage areas at the Port facility, a security plan shall describe the *nuclear security* arrangements that meets the requirements set out in paragraph 2.4.

2.2. The security plan shall include diagrams and specifications of the security infrastructure that identifies the layout of security boundaries and the position of any security equipment including cameras, detection devices and access control features.

2.3. The Permit Holder shall obtain *Director General's* approval of the security plan prior to storage incidental to transport.

2.4. A land-side secure storage is a separately enclosed area protected by a barrier consisting of either a security fence or building fabric or other barrier, with access control and:

a) the presence of 24 hours security guard(s) or other authorised personnel; or

b) a high assurance of detection by remote surveillance; or

c) a combination of the above; and

d) access to *TEU* containers are to be restricted to authorised persons who require it.

3. Emergency Procedures

3.1. The Permit Holder shall implement procedures:

3.1.1. to maintain adequate *nuclear security* in the event of delayed shipping, or accident involving *UOC*;

3.1.2. to provide for a timely and effective response in the event that theft, loss or unauthorised handling of *nuclear material*.

4. Reports, Notifications and Requests for Approvals

4.1. The Permit Holder or *Designated Individual* shall report to, notify or apply to the *Director General* as appropriate for each activity or item listed in section 5.

4.2. Each such report, notification or application shall be made by completing the specified forms listed in section 5 or using other formats as approved by *ASNO*.

4.3. The reports, notifications or applications shall be delivered to the *Director General* in accordance with the reporting requirements specified on the respective form.

5. ASNO Forms

Forms are reviewed or amended from time to time. Current forms can be downloaded from the *ASNO* website at: www.dfat.gov.au/asno

5.1. Approval forms

APPLICATION FORMS TO CONDUCT CERTAIN ACTIONS:[1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Application to Create a New Approved Location	- 7 day notice	ASO112
Change to the Accountancy or Security Plan		ASO134

5.2. Notification forms

NOTIFICATION IS REQUIRED FOR: [1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Notification of an Incident	- Report *incidents* by phone within 2 hrs. of detection - submit form within 4 hrs.	ASO201
Notification of Designation of an Individual		ASO214
Notification of Change to Permit Holder's Particulars	- Within 10 days of effect of change	ASO231

[1] Each report, notification or application should be made by the *Permit Holder's Representative* or by a *Designated Individual* as notified under ASO214, responsible for compliance with that application requirement.
[2] Refer to related form for detailed timeframe requirements. All days refer to consecutive business days.

5.3. Report Forms

REQUIRED REPORTS:[1]	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING:[2]	FORM TO USE:
Report on Incident Investigation	- Within 30 days of initial report	ASO303

6. Nuclear Security - Scalable Threat Model

6.1. The purpose of the scalable threat model is to establish a system of standardised maritime transport protection measures for a wide range of security threats and their resultant risks to the production and subsequent handling of *UOC*. The scalable model's categories prescribe levels of transport protection measures that shall be implemented for each of the different levels of threat and resultant risks.

6.2. The Permit Holder should be able to implement a scalable system of interim measures that collectively address changes in threat levels and their associated risks. These measures shall be capable of being implemented rapidly in response to an elevated threat, and for the system to remain cost effective, it is desirable that the interim measures be readily discontinued.

6.3. The Permit Holder shall at all times, be able to operate at, and maintain, MARSEC 1, 2 and 3 measures, as appropriate. The Permit Holder should respond to any threat to *UOC* by raising their security measures to comply with the appropriate MARSEC security level.

6.4. The Director General shall be informed of any escalated incident for above-mentioned procedures.

Table 1: Maritime Security Threat Level Scale

Maritime security level	Environment	Measures
MARSEC 1	Normal business operations	Minimum protective *security* measures should be maintained at all times
MARSEC 2	Heightened risk of a *security* incident	Targeted measures implemented during period of heightened risk
MARSEC 3	A *security* incident is probable or imminent	Although a specific target may not be known, further *security* measures must be maintained while the *security* incident is probable or imminent

[1] Each report, notification or application should be made by the *Permit Holder's Representative* or by a *Designated Individual* as notified under ASO214, responsible for compliance with that application requirement.
[2] Refer to related form for detailed timeframe requirements. All days refer to consecutive business days.