



COMPLIANCE CODE FOR CLASS U3 PERMITS

Compliance Code History

Version	Date of Effect	Description
1	30/09/2016	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*, *Nuclear Security* and for Nuclear Material Transport Plans for all Class U3 Permits to Transport *Nuclear Material* issued under section 16 of *the Act*. It also sets out forms for the submission of applications, notifications and reports.

Where individual criteria or requirements of the *Compliance Code* cannot be met, *ASNO* may accept alternate compensatory measures if they provide an equivalent level of *nuclear security*. Such alternate measures shall be explicitly addressed in the Nuclear Material Transport Plan and must be approved by the *Director General*.

Scope

This *Compliance Code* applies to Permits identified under paragraph 3 of the Permit as a Class U3 permit. The requirements of the *Compliance 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 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*.

For the purpose of this *Compliance Code*, *nuclear security* will be taken to apply to *nuclear material* (including *UOC*) but not to other radioactive materials.



1. Risk Assessment

The Permit Holder shall conduct and document a risk assessment for any specific security threats to *UOC* relevant to the Permit Holder.

Guide: It is preferable that risk assessments are done according to AS/NZS ISO 31000:2009 or an applicable industry standard.

2. Nuclear Material Transport Plan (The Plan)

2.1. Transport Governance

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 a system for *nuclear material* control and *nuclear security* in its possession that addresses the conditions in the Permit and the current *Compliance Code* or any other instruction authorised in writing by the *Director General*.

The system for the control and security of *nuclear material* shall at all times be described in documented *Plans* and arrangements. The Permit Holder shall:

- 2.1.1. appoint responsibilities for the activities involving *UOC* and clearly define the scope of each responsibility;
- 2.1.2. produce or adopt a *Plan* covering the transport and any storage incidental to transport, addressing the risks identified in section 1, including scalable nuclear security measures and procedures capable of being implemented rapidly in response to identified elevated threats. The scalable threat model shall be linked to the Maritime Security Threat Level Scale (MARSEC) as applicable.
The Plan may be an exclusive *Plan* or incorporated into plans compiled for other purposes;
- 2.1.3. implement all measures specified in *The Plan*;
- 2.1.4. review *The Plan* at least once during the term of this Permit, or at the request of the *Director General*, or as required to respond to changes in circumstances, whichever is the sooner;
- 2.1.5. restrict access to information about *The Plan* and auxiliary security information except to persons with a need-to-know, ensuring dissemination accordingly. *The Plan* shall be labelled (header and footer) with protective markings commensurate with its sensitivity (e.g. "Sensitive - Security").



2.2. Control Measures

The Permit Holder shall:

- 2.2.1. detect any *loss of control of nuclear material* listed on the *manifest*;
- 2.2.2. maintain organisational arrangements enabling the Permit Holder to determine the precise location of any material on the Permit Holder's *manifest* or in storage incidental to transport, in less than 2 hours;
- 2.2.3. keep an up-to-date ledger of all *nuclear material* transferred to and from the Permit Holder, recording details for each separate receipt and delivery, for a period of 5 years after the last entry therein; and
- 2.2.4. ensure that *TEU* containers of *nuclear material* are individually labelled as on the Permit Holder's *manifest*, with unique identification markings in a way that enables timely matching for verification;
- 2.2.5. maintain the integrity of tamper indicating devices (e.g. seals) ensuring that after any access by Port Authorities, tamper indicating devices have been reapplied; and
- 2.2.6. The Permit Holder shall notify the *Director General* if the vessel does not have or is not required to have a Ship Security Plan.

2.3. Route

The Permit Holder shall transport the *nuclear material* only by approved vessel(s) for transportation and along approved transport route(s):

- 2.3.1. specified in the consignor Application for Permit to Transport Nuclear Material; or
- 2.3.2. otherwise nominated by the consignor, and approved by the *Director General* (Application form ASO113).

2.4. Transport Arrangements

During sea transport the Permit Holder shall:

- 2.4.1. preferentially place *TEU* containers below deck as a Bay Plan requirement;
- 2.4.2. adopt appropriate measures to minimise any risks identified in section 1 on the approved route(s);
- 2.4.3. meet specific requirements of the *Director General* in areas of high-risk piracy¹;

¹ For the Gulf of Aden this means the area defined as the High Risk Area by the United Kingdom Marine Trade Operations. For other areas this means the Listed Areas as published by the Joint War Committee.



- 2.4.4. deliver the *nuclear material* only to the consignee or authority at the port of discharge specified by the consignor; and
- 2.4.5. implement recovery procedures in case of any *loss of control of nuclear material*.

2.5. Storage Incidental to Transport

- 2.5.1. *The Plan* shall describe the *nuclear security* arrangements for portside or land-side storage incidental to transport of *UOC*, where under the control of the Permit Holder.
- 2.5.2. The *security* of *TEU* containers holding *UOC*, stored prior to shipment in Australia shall meet the requirements of the current relevant port MARSEC threat level.

3. Reports, Notifications and Requests for Approvals

- 3.1. 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 4.
- 3.2. Each such report, notification or application shall be made by completing the specified forms listed in section 4 or using other formats as approved by *ASNO*.
- 3.3. The reports, notifications or applications shall be delivered to the *Director General* in accordance with the reporting requirements specified on the respective form.

4. 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

4.1. Approval forms

APPLICATION FORMS TO CONDUCT CERTAIN ACTIONS: ¹	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING: ²	FORM TO USE:
Application to Use a Vessel to Ship Uranium Ore Concentrates (UOC)	- 7 day notice	ASO111
Application to Approve a New (or Variation to a Current) Transport Plan	- 20 day notice for new route	ASO113
Application to Subcontract Functions Subject to Permit Restrictions and Conditions	- 14 day notice	ASO135

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.



4.2. Notification forms

NOTIFICATION IS REQUIRED FOR: ¹	TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING: ²	FORM TO USE:
Notification of an Incident	- Report <i>incidents</i> 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

4.3. 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

5. Nuclear Security - Scalable Threat Model

- 5.1. 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.
- 5.2. *The Plan* should include 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.
- 5.3. 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.

Table 1: Maritime Security Threat Level Scale

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