COMPLIANCE CODE FOR CLASS U1 PERMITS

COMPLIANCE CODE HISTORY

Version	Date of Effect	Description
1	31/03/2018	*Compliance Code* first issue
2	30/03/2023	This variation: - Issue of new template U1 *Compliance Code* 3.2 - Appointment of individuals assigned defined responsibilities 4.2.3 - New condition – Ad hok request for *inventory* taking 13.4 - Document, control and dispose of IT for EACS and *MC&A* 14.5 - NTTAS level downgraded from Probable to Possible 17 - New section on incident reporting 18.2 - New text to articulate an existing requirement by ASO106 18.4.1- Additional tabs to better identify individual requirements 19.1 - New ASO112 form heading 21 - Definitions relocated from U1 Permit to this section.

PURPOSE

The purpose of this *Compliance Code* is to establish a standard set of requirements for the systems of *Material Control and Accountancy* and *Nuclear Security* for all Class U1 Permits to Possess Nuclear Material issued under section 13 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 those measures provide an equivalent level of *nuclear security*. Such alternate measures shall be explicitly addressed in *the Plan* and must be approved by the *Director General*.

SCOPE

This *Compliance Code* applies to Permits to Possess Nuclear Material issued under section 13 of *the Act* identified under paragraph 3 of the Permit as a Class U1 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*.

OBJECTIVES

The objectives of the systems for Nuclear *Material Control and Accountancy* 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 minimise 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 include other radioactive materials.

1. MANAGEMENT SYSTEMS

The Permit Holder's management system addressing the requirements of this *Compliance Code* shall encompass:

1.1. risk management;

1.2. training and awareness;

1.3. use of good practice and lessons learned from experience;

1.4. internal review and performance assessment;

1.5. organisational management structure that defines the responsibility, authority and the interrelationship of personnel; and

1.6. programs to maintain an effective *security culture* at all levels throughout the organisation.

2. RISK ASSESSMENT

2.1. The Permit Holder shall conduct and document a risk assessment that takes into account the consequences of sabotage and identifies specific security threats to *UOC*, both new or changed, relevant to the Permit Holder.

> Guide: It is preferable that risk assessments be conducted according to AS ISO 31000:2018 or an applicable industry standard.

3. PLANS AND PROCEDURES (THE PLAN(S))

The Permit Holder shall:

3.1. maintain systems for *nuclear security* and *material control and accountancy.* These systems shall:

3.1.1 address conditions in the Permit and the current *Compliance Code* including appendices, or any other instruction authorised in writing by the *Director General; and*

3.1.2 be described in documented *plans*, procedures and arrangements.

3.2. Appoint persons and clearly define the scope of their responsibilities for activities involving *UOC*;

3.3. produce or adopt *Plan*(*s*) covering *nuclear security*, *material control and accountancy*, transport and any storage incidental to transport, addressing the current risks identified in section 2 of this *Compliance Code*, 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 Australian Security Intelligence Organisation (*ASIO*) National Terrorism Threat Advisory System (NTTAS) levels as described in section 14 of this *Compliance Code* as applicable;

3.3.1 *Plan*(*s*) may be incorporated into plans compiled for other purposes;

3.4. obtain *Director General's* approval for these *Plan*(*s*) prior to the commencement of activities involving *UOC* allowed by this Permit;

3.5. implement all measures specified in these *Plan*(*s*);

3.6. review these *Plan*(*s*) 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 and:

3.6.1 inform the *Director General* of the detail and outcome of these reviews; and

3.6.2 as required, make application for proposed changes to these *Plan*(*s*), or advise that no changes were assessed as necessary; and

3.7. restrict access to *Plan*(*s*) or auxiliary *security* information to persons with a need-to-know and disseminate to those who do. *Plan*(*s*) shall be labelled (header and footer) with protective markings commensurate with the level of sensitivity (e.g. "OFFICIAL: Sensitive").

4. CONTROL MEASURES

The Permit Holder shall:

4.1. detect any *loss of control* of *UOC* listed on the Permit Holder's *inventory*;

4.2. maintain organisational arrangements to enable the Permit Holder to:

4.2.1 detect within 7 days any *loss of control* of *UOC* listed on the *inventory* ;

4.2.2 determine in less than 2 hours the precise location of any *UOC* on the Permit Holder's *inventory* or in storage incidental to transport; and

4.2.3 report to the *Director General* upon request, the *inventory* of *UOC* held, in transit and in storage incidental to transport;

4.3. establish measures and procedures to ensure access to *UOC* is only granted to:

4.3.1 persons authorised by the Permit Holder;

4.3.2 non-authorised persons escorted by a person authorised to escort;

4.3.3 *ASNO inspectors* and *Agency inspectors*; or

4.3.4 persons responding to an emergency or *security* event consistent with the Permit Holder's emergency plan; and

4.4. provide an effective and timely internal procedure for reporting *security* incidents.

5. NUCLEAR SECURITY SYSTEM

A Nuclear Security System comprises effectively integrated detection with assessment, access delay, and timely response, realised through personnel, procedures, physical structures, hardware, equipment and the application of prudent management practices and information security.

5.1. Specifically, for the purpose of protecting *UOC* at *Approved Locations*, *ASNO* requires, inter alia, that local arrangements be in place that will:

5.1.1 provide timely detection and assessment of *security* significant events;

5.1.2 delay access to an adversary through installation of elements including fences, gates, building fabric or other barriers; and

5.1.3 initiate an appropriate response within ten minutes of the detection.

5.2. To ensure the optimal performance of the *security* system, the Permit Holder should incorporate the *nuclear security* system into existing quality assurance programs.

5.3. It is preferrable that any protective security equipment used be endorsed by the Security Construction and Equipment Committee (*SCEC*), as produced by the Australian Security Intelligence Organisation in the Security Equipment Evaluated Product List (*SEEPL*).

5.4. The Permit Holder shall provide for a central alarm station (CAS) function to undertake complete and continuous alarm monitoring, assessment and communications with guards, facility management and the response/police forces.

6. SECURE COMPOUND

6.1. A Secure Compound is an enclosed area protected by a barrier consisting of either a security fence or building fabric or other barrier, with access control; and

6.1.1 the presence of 24 hour security guard(s) or equivalent arrangement; or

6.1.2 other measures to achieve a high assurance of detection and assessment of unauthorised access with a timely initiation of response.

6.2. For a Secure Compound, the following shall apply:

6.2.1 access control may be implemented by either an electronic access control system or mechanical locking approved by the *Director General*;

6.2.2 access is to be restricted to authorised persons who require it;

6.2.3 assessment and verification of alarm detection shall be achieved through monitored closed circuit television (CCTV) camera(s) or visual oversight by security guard(s) or other authorised personnel;

6.2.4 performance of cameras, monitors and the illumination of the area, shall enable the assessment of a person or activity being monitored during day and night;

6.2.5 where mechanical locking is used, keys are to be strictly controlled by an appointed officer and secured when not in use; and

6.2.6 records are to be kept of electronic access control or the issue of keys.

6.3. For security fences, gates and barriers, the Permit Holder shall:

6.3.1 Install internal security fences and gates to Australian Standards (specifically, AS/NZS 1725.1-2010: Chain link fabric - Security fences and gates - General Requirements) and provide the following performance:

a) fences shall include anti-climb measures and have a minimum total height of 2.4 metres above ground level; and

b) installation of structures or placement of items shall not be closer than two metres of the perimeter of the fence or gate. Where existing infrastructure forms a climbing aid, or is within two metres of the perimeter of the fence or gate, compensatory measures shall be installed;

6.3.2 mount additional fence fabric to mitigate against entry/exit via ditches, drains or by tunnelling under the fence, or where anti-climb measures are circumvented;

6.3.3 install gates and other barriers which provide at least the same level of protection as provided by the fence. Power operated gates should have manual override and/or emergency power-back-up features;

6.3.4 perform inspections, ensure maintenance of good repair and remove equipment, structures or materials that could aid unauthorised ingress; and

6.3.5 ensure that main entry gates are overlooked by staffed guarding posts, or monitored CCTV; or otherwise secured if unattended.

7. BASELINE LEVEL NUCLEAR SECURITY MEASURES

The conditions below constitute the baseline *nuclear security* measures to be applied to uranium in process, *UOC* in storage and functions under normal operating conditions. *UOC* is not to be stockpiled or stored outside of the areas described in sections 7.3 to 7.5 of this *Compliance Code,* without the written authority of the *Director General* and only if an appropriate level of *nuclear security* is maintained for this material.

7.1. Satellite Production Areas (where applicable)

The following *security* provisions shall apply to any satellite production area that contains uranium in process which will be delivered to the main production area for final production of *UOC*:

7.1.1. A single fence surrounding satellite areas, having a minimum height of 1.8 metres;

7.1.2. access to the area shall be controlled; and

7.1.3. a register shall be kept of deliveries from the satellite production area to the main processing plant.

7.2. **Pre-Precipitation Areas**

7.2.1 Production areas that contain uranium in process shall:

a) be located wholly within the *Approved Location*; and

b) apply prudent measures and controls to prevent unauthorised access to uranium in process.

7.3. **Precipitator and Product Thickener Plant Area(s)**

7.3.1 An access controlled area consisting of at least one physical barrier (security fence, building fabric or otherwise) shall be used to only allow access to authorised persons; and

7.3.2 access to *UOC* product thickener plant sample points/taps shall be controlled to either detect and/or hinder unauthorised activities (e.g. by monitoring, mechanical locking, restricted access or otherwise).

7.4. **Centrifuge, Calciner/Dryer and Drum Filling Area(s).**

7.4.1 This area (or areas) shall meet the requirements for a secure compound, with two segregated barriers between the general site area and areas containing *UOC*, each with access control (e.g. a building within a fenced compound);

7.4.2 Drum filling activities shall at all times be monitored by authorised personnel or by CCTV camera monitoring; and

7.4.3 Unsupervised drums of *UOC* shall be stored in a manner to hinder, and allow detection and assessment of, unauthorised activities (e.g. by CCTV monitoring, mechanical locking, or otherwise).

7.5. **Packing**

7.5.1 *UOC* shall be packed in IP-1 205 litre open-head mild steel drums, or other packaging as approved by the *Director General*.

7.5.2 For shipment, sealed drums shall be loaded into standard ISO 20 or 30 tonne rated, 20-foot ISO shipping containers (*TEU*).

7.5.3 Each container shall be secured with locks or container seals of a type approved by the *Director General*; and

a) once final checks have been completed, consecutively numbered container seals shall be applied before the containers are transported off-site; and

b) put procedures in place to control and track tamper indicating devices for each shipping container.

The Permit Holder may seek permission from *the Director General* to transport *UOC* in containers (7.4.2) during transport to Port with hardened padlocks to *SL3* security level rating (5.3), for the purposes of quality control. Containers are to be sealed in accordance with (7.4.3) prior to transferring the consignment to port authorities/stevedores.

7.5.4 Ensure that *TEU* containers of *UOC* are individually labelled as on the Permit Holder's *manifest*, with unique identification markings that permit timely matching for verification.

7.5.5 Arrange an agent for each port of loading and unloading, including trans-shipment, to provide oversight of the containers. The agent shall check that the integrity of the containers and seals and report the result of such checks to the *Director General*.

7.6. **UOC Storage Compounds**

7.6.1 Drums containing *UOC* stored outside the drum filling area shall be secured in shipping containers in secure compounds in accordance with section 6 of this *Compliance Code*.

7.6.2 Preferably, sealed containers will be placed in the compound(s) in *door-facing-door* configuration or otherwise arranged to prevent the opening of container doors; or, if this is not operationally practical, the containers shall be positioned to enable detection and assessment of attempts at unauthorised access to the container doors.

7.7. **UOC Sample Storage**

7.7.1 *UOC* or other in-process uranium, as samples, shall be securely stored in access controlled areas to either detect and/or hinder unauthorised activities (e.g. by CCTV monitoring, mechanical locking, or otherwise); and

7.7.2 records are to be kept of electronic access control or the issue of keys.

8. MAINTENANCE, TESTING AND INSPECTIONS

8.1. The Permit Holder shall ensure all *security* related equipment is inspected and maintained to ensure continued effectiveness.

8.2. Performance of the *nuclear security* system shall be periodically tested (at least annually) to ensure its continued effectiveness.

8.3. Should *security* deficiencies be identified, the Permit Holder shall ensure that corrective actions are taken in a timely manner commensurate with the security risk.

9. COMPENSATORY MEASURES

9.1. Whenever the *nuclear security* system is determined to be incapable of providing the required level of protection, the Permit Holder shall promptly implement compensatory measures to provide adequate protection.

9.2. For significant *security* events, the Permit Holder shall inform *ASNO* of the implementation and removal of compensatory measures.

10. **SUBCONTRACTING OR OUTSOURCING SECURITY ACTIVITIES INVOLVING UOC**

If the Permit Holder is *subcontracting* a *security* function to a person who is not another Permit Holder, the Permit Holder's *security* requirements are to be identified and included in the contract. These contracts, where relevant, shall provide for:

10.1. written confidentiality agreements between the *subcontractor* and the Permit Holder; and

10.2. *security* performance indicators/reports, subject to review, for contract terms greater than 2 years.

11. **STAFF, SUBCONTRACTORS AND VISITORS**

The Permit Holder shall ensure that:

11.1. all staff and *subcontractors* in access controlled areas carry, produce on demand, and preferably display security passes or other valid site-issued identification;

11.2. site security staff are informed immediately of staff or *subcontractors* no longer requiring access to controlled areas (e.g. due to resignation or completion of contract) to ensure that security passes are returned and access privileges are revoked;

11.3. visitors within access controlled areas are escorted at all times and are issued with a current visitor's pass which shall be recovered following completion of the visit; and

11.4. a contact reporting scheme is in place for staff and *subcontractors* to report approaches by any person inappropriately seeking information of a security sensitive nature.

12. **SECURITY RECORDS**

12.1. The Permit Holder shall ensure that *security* related records associated with the operation of the security monitoring system are maintained and made available to an *inspector* on request.

12.2. All electronic access control records, event-triggered CCTV images of alarm events (excluding those triggered from authorised access), alarm event and response logs, security maintenance records, paper based records (e.g. sign in/sign out records, security patrol and *security* incident logs) etc, are to be held for a minimum of 12 months.

12.3. Continuous CCTV recordings are to be held for a minimum of 30 calendar days.

13. **NETWORKED INFORMATION TECHNOLOGY SYSTEMS**

The Permit Holder shall protect any networked information technology (IT) system including remote access to the IT system, used to protect *UOC*, and shall include the following functions:

13.1. the recording of network logon attempts;

13.2. protocols in place allowing timely disabling of the ex-staff member's IT network account; and

13.3. a password management system that; forces a minimum password length, forces staff to regularly change passwords, locks terminals after a number of failed password attempts, and locks terminals after a period of computer inactivity.

13.4. Document, control and appropriately dispose of IT system hardware used for the protection of *UOC* (eg. electronic access control) or used for *MC&A* recording of *UOC inventory.*

14. **SCALABLE THREAT MODEL - SCALABLE NUCLEAR SECURITY MEASURES**

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

14.2. *Plan(s)* should include a scalable system of interim measures that collectively address changes in threat levels and 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.

14.3. Five *security* threat levels, identified below for uranium mines and associated transport, are related but not equivalent to the Australian Security Intelligence Organisation (*ASIO*) National Terrorism Threat Advisory System (NTTAS) levels. The *Director General* will notify the Permit Holder of the *security* threat level that applies at any given time after having received advice from *ASIO* and/or law enforcement authorities.

14.4. The Permit Holder is required to defend against the identified level of threat, which is specified in table 1 and to provide sufficient *nuclear security* measures specified in table 2 below.

14.5. Table 1: Threat Levels

NTTAS	Description
Not Expected	There is no indication of any *security* threat to mine activities; This level is the baseline uranium mining threat level[1]
Possible	There is no specific *security* threat targeted towards mine activities (limited intent or capability)
Probable	There are concerns of a heightened threat and mine activities should exercise a high degree of caution
Expected	There are *security* concerns of a threat with intention and capability planned against mine activities
Certain	A specific *security* threat is certain or underway

14.6. Table 2: Scalable Nuclear Security Measures

14.6.1 **Not Expected**
This level of threat represents the minimum threat posed and the conditions constitute the baseline *nuclear security* measures to be applied for the storage and transport of *UOC* and its process and functions under normal operating conditions.
In addition to baseline *security* measure applicable at the **NOT EXPECTED** threat level, the following requirements apply at elevated threat levels. Further to the measures stipulated below, the Permit Holder may also propose additional measures at **POSSIBLE** and **PROBABLE** threat levels:

[1] At time of issuing this permit, the national terrorism threat levels was set at POSSIBLE, however the specific threat level set for uranium mining activities is NOT EXPECTED. The *Director General* will inform permit holders of any changes to mining threat level assessments.

14.6.2 **Possible**

Description	Site Storage Arrangements	Arrangements for Transport/ Storage Incidental to Transport
This level applies when attack against the Permit Holder's infrastructure or activities is assessed as feasible and could well occur. This level can be issued by the *Director General*, on the advice of *ASIO* or the Australian Federal/State/ Territory Police (*AFP*). It is possible that once this level is implemented it may remain for several years. Maintain all NOT-EXPECTED level requirements and the following treatment measures shall be implemented:	a) Increased liaison with local Police. b) Increased guard presence at storage sites to allow regular site patrols and effective monitoring of *security* systems whilst retaining timely assessment of alarm events. c) Increased oversight of staff and *subcontractor* activities associated with the *UOC* process. d) Maintain high degree of vigilance and *security* awareness.	e) Provide constant GPS tracking of all *UOC* road/rail transports. f) Provide driver(s) with escalated risk contingency including approved alternate transport route(s) or return of consignment options. g) Single vehicle transport shall be accompanied by a support vehicle. h) Provide accurate and concise information for a diligent emergency response.

14.6.3 **Probable**

Description	Site Storage Arrangements	Arrangements for Transport/ Storage Incidental to Transport
This level applies when an attack against the Permit Holder's infrastructure or activities is assessed as likely. It is possible that once this level is reached it may remain up to 12 months. Maintain all NOT-EXPECTED and POSSIBLE level requirements and the following treatment measures shall be implemented:	a) Increase frequency of verification of tamper indicating devices b) Increased access control, entry checks, including to vehicles allowed on-site c) Increased patrols where *UOC* is stored during operational hours; or d) full time guarding of *UOC* during non-operational hours.	e) In consultation with *AFP*, *ASIO*, *ASNO*, and local Police develop and identify, where possible, alternate road transport routes and arrangements that provide a higher degree of assurance for safety and *security* f) Road transport to have an armed escort, with guard presence at loading and unloading of shipping containers g) Increase driver reporting and decrease passive GPS waypoint reporting distances h) Store *UOC* only in secure compound i) Increase frequency of verification of tamper indicating devices

14.6.4 **Expected**		
Description	**Site Storage Arrangements**	**Arrangements for Transport/ Storage Incidental to Transport**
This level of *security* applies when attack against the Permit Holder's infrastructure or activities is assessed as imminent. At this level, there is credible specific intelligence of planned sabotage or theft of *UOC*. It is expected that this level would be applied for short periods (e.g. 30 days or until the threat is dealt with). The following measures shall apply:	a) The *Director General* will brief the Permit Holder on the situation, the Permit Holder decides whether to continue production or handling of *UOC* at the *Approved Location* b) The Permit Holder will continuously monitor the location and quantity of all *UOC* in its control and immediately notify the *Director General* of any changes c) If the specific intent of the threat is understood at the time, risk reduction measures may require flexibility to obtain the best outcome. This will require continuous liaison and cooperation with the *Director General*, and potentially other stakeholder agencies and law enforcement bodies d) Understanding the specific threat intent at the time, flexibility in risk reduction measures may obtain the best outcome, requiring continuous liaison and cooperation with the *Director General*, stakeholder agencies and law enforcement bodies.	e) When this level is raised, unload *UOC* shipments in transit at the nearest approved secure compound. f) Note: the *Director General* may require shipment of *UOC* to a more secure location and determine if an armed escort is required. g) All movements of *UOC* are to cease. *UOC* is to remain in secure compounds. Loaded *TEU* containers are to remain in the sealed condition and placed in *door-facing-door* configuration. h) The Permit Holder will continuously monitor the location and quantity of all *UOC* in its control and immediately notify the *Director General* of any changes.

14.6.5 Certain

This level of *security* applies when attack against the uranium industry or activities is imminent or occurring (Riots, looting, intrusion or heist). At this level, planned sabotage or theft of *UOC* is in progress or being perpetrated.

This level is evident by the attack or is issued by the *Director General*, *ASIO*, local Police and/or the *AFP*. It is expected that this level would be applied for short periods (e.g. hours/days or until the threat is dealt with).

All persons are to make every effort to preserve life and prevent violent conflict.
(Personal safety has priority over the protection of *nuclear material*.)

15. MATERIAL CONTROL AND ACCOUNTANCY (MC&A) SYSTEM

The *plans* and procedures referred to in section 3.2 of this *Compliance Code* shall include an *MC&A* Plan covering *nuclear material* during use, transport and storage that meets the objectives specified in this *Compliance Code*. The system of accountancy shall:

15.1. Maintain accurate, timely, complete, and reliable information on the characteristics and disposition of uranium in all forms in the facility's possession, including all uranium received, extracted, produced, lost or otherwise removed from *inventory*;

15.2. provide for the timely investigation and resolution of any accounting anomaly indicating a possible loss of *UOC*, assisting in determining if unauthorised removal has actually occurred and conducting an emergency *inventory* taking, if required;

15.3. enable the timely and accurate preparation of accountancy reports required by this Permit;

15.4. make measurements in accordance with the requirements of section 16 of this *Compliance Code*, noting all factors that adversely impact the ability to meet these requirements (e.g. presence of high humidity);

15.5. determine the precision and accuracy of measurements and estimate measurement uncertainties;

15.6. where measurement uncertainties do not meet the target values in section 16 of this *Compliance Code*, modify the measurement system so that the targets can be achieved, compensating for all measurement constraints as much as is reasonably possible;

15.7. minimise shipper/receiver differences over time;

15.8. record the movement of *UOC*, including samples, between distinct locations and custodians;

15.9. record any *inventory* change on the day the change occurs or is calculated at the operational level;

15.10. locate precisely a particular item on the Permit Holder's *inventory* in less than 2 hours;

15.11. notify the *Director General* of any consignment of *UOC* in storage incidental to transport that is held in any one location within Australia and outside of the *Approved Locations* as specified in paragraph 9 of the Permit U1, for a period longer than 30 calendar days;

15.12. conduct a physical *inventory* taking of *UOC* not more than 30 calendar days prior to and no later than 30 June and 31 December each year;

15.13. report mining activities to *ASNO* by completing form ASO324 by 15 March describing operations up to 31 December of the previous year; and

15.14. retain records of holdings and transfers of *nuclear material* for a period of 5 years.

16. MEASUREMENTS OF URANIUM ORE CONCENTRATE ("UOC")

16.1. Weighing of *UOC* shall be determined using equipment and procedures with an overall measurement uncertainty (random and systematic) less than or equal to 0.1%, noting that drums shall be tared to plus or minus 200 grams.

16.2. The procedure selected for sampling *UOC* shall ensure maximum representativeness, to achieve the overall measurement uncertainty in section 16.3 of this *Compliance Code.*

16.3. Determination of uranium in *UOC* shall have an overall measurement uncertainty (random and systematic) of less than or equal to 0.2%[1]. The analytical sample used for this determination shall be in the same state of dryness as the sample used for moisture analysis, at the conclusion of the loss-on-drying measurement.

16.4. The units for measurements shall be recorded to two decimal places:

16.4.1 All weights shall be recorded in kilograms; and

16.4.2 Both moisture and contained uranium in *UOC* shall be recorded as percentages.

17. INCIDENT REPORTING

The Permit Holder shall promptly notify the *Director General* within 2 hours of detection of each incident in accordance with Form ASO201, pertaining to:

17.1. a *loss of control* including actual, attempted or suspected theft, loss or compromise of *nuclear material*;

17.2. an unauthorised access to or use of *nuclear material*; or

17.3. a failure of the *security* measures.

18. REPORTS, NOTIFICATIONS AND REQUESTS FOR APPROVALS

18.1. 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 19 of this *Compliance Code*.

18.2. The permit holder shall obtain *ASNO* approval for all international or domestic transfers of *nuclear material* from or to the Permit Holder.

18.3. Each such report, notification or application shall be made by completing the specified forms listed in section 19 or using other formats as approved by *ASNO*.

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

[1] Measurement uncertainties refer to the 95% confidence level that the measured weight does not differ from the true weight by more than the number quoted.

18.4.1 The Permit Holder shall not engage any act until receiving approval (even if the approval surpasses the timeframe limit).

19. ASNO FORMS

The Permit Holder shall use the forms listed in sections 19.1-19.3 of this *Compliance Code,* available at www.dfat.gov.au/asno (as amended from time to time) or the equivalent on *ASNO*'s online portal (the NUMBAT database portal https://numbat.dfat.gov.au).

19.1. Approval Forms

APPLICATION FORMS TO CONDUCT CERTAIN ACTIONS:[1]	**TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING**:[2]	**FORM TO USE**:
Application to Transfer Material (Import, Export or Domestic Transfer)	- 7 day notice	ASO106
Application to Consume, Dilute or Dispose of Nuclear Material or Associated Item [3]	- 7 day notice	ASO108
Application to Transfer Uranium Ore Concentrates (UOC) Internationally	- 7 day notice[4]	ASO110
Application to Use a Vessel to Ship Uranium Ore Concentrates (UOC)	- 7 day notice	ASO111
Application to Create or Remove an Approved Location	- 7 day notice	ASO112
Application to Approve a New (or Variation to a Current) Transport Plan	- 20 day notice – new route - 10 day notice – modified transport plans	ASO113
Application for Approval of Changes to the Accountancy or Security Plan	- 10 day notice	ASO134
Application to Subcontract Functions Subject to Permit Restrictions and Conditions	- 14 day notice	ASO135
Application for Approval to Export UOC to Bulk Overseas Converters (Include ASO110)	- Annual application - 20 day notice	ASO136

[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. For events requiring approval forms, the event must not take place before *ASNO* approval is granted.

[3] *Nuclear material* may only be disposed of in such a way that the *nuclear material* will become practicably irrecoverable.

[4] 7-day notice only applies to transfers undertaken pursuant to prior approved ASO136 forms in this regard. All other transfers require increased notice periods, typically beyond 30 days.

19.2. Notification Forms

NOTIFICATION IS REQUIRED FOR: [1]	**TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING**:[2]	**FORM TO USE**:
Notification of an Incident	- Report *incidents* to ASNO by phone within 2 hours of detection - Submit form within 4 hrs.	ASO201
Notification/Confirmation of UOC Discharge and Arrival Details	- 2 day packing notice prior to export or after receiving bills of lading serial no. - Departure date confirmed by 12 pm next day - Within 7 days of each change of custody	ASO203
Notification of Final Data Certificates from a Receiver	- Upon request	ASO212
Notification of Designation of an Individual		ASO214
Notification of Change to Permit Holder's Particulars	- Within 10 days of effect of change	ASO231
Acknowledgement of Receipt of Sealed Goods	- Within 4 hours of courier receipt - Provide copy of shipping docs. within 2 days	ASO232

19.3. Report Forms

REQUIRED REPORTS:[1]	**TIMEFRAME LIMITS FOR APPLICATIONS, NOTICE OR REPORTING**:[2]	**FORM TO USE**:
Inventory Balance Report (Uranium Ore Concentrate – UOC)	- Biannual reporting - Within 15 days of reporting period	ASO301
Report on Incident Investigation	- Within 10 days of initial report	ASO303
Report on Mining Activities	- Annual reporting - By 15 March reporting on previous year	ASO324

[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.

20. **TABLE: DOCUMENTS RELATED TO MANAGING COMPLIANCE WITH CONDITIONS IN THIS PERMIT.**

Last updated: 16 January 2018

Document Short Name	DocumentFull Name or Description
SEEPL	The Security Equipment Evaluated Product List (*SEEPL*), as produced by Security Construction and Equipment Committee (*SCEC*) of the Australian Security Intelligence Organisation.
AS/NZS ISO 31000: 2018	Risk management - Principles and guidelines
AS/NZS 1725.1: 2010	Chain link fabric fencing Security fences and gates - General Requirements

NOTE: *Subject to the Administrative Appeals Tribunal Act 1975 and to sub-section 22(8) of the Nuclear Non-Proliferation (Safeguards) Act 1987, application may be made to the Administrative Appeals Tribunal, by or on behalf of a person whose interests are affected by a decision by the Minister, pursuant to sub-section (2) of section 13 of the Act, imposing a condition or restriction on the grant of a Permit, for review of the decision.*

21. **DEFINITIONS**

Act (the)	Means the *Nuclear Non-Proliferation (Safeguards) Act 1987*.
Additional Protocol	Means the Protocol Additional to *the Agency Agreement* (INFCIRC/540), that entered into force on 12 December 1997.
AFP	Means the Australian Federal Police.
Agency (the)	Means the International Atomic Energy Agency (IAEA).
Agency Agreement	Means the Agreement between Australia and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons (INFCIRC/217), being the Agreement which was signed on behalf of Australia on 10 July 1974, a copy of which is set out in Schedule 3 of the Act.
Agency Inspector	Means a person declared to be an inspector of the International Atomic Energy Agency pursuant to section 57(2) of *the Act*.
ASIO	Means the Australian Security Intelligence Organisation.
ASNO	Means the Australian Safeguards and Non-Proliferation Office.
ASNO Inspector	Means a person appointed to be an inspector pursuant to section 57(1) of *the Act*.

Compliance Code(**s**)	Means the document called "Compliance Code for Class U1 Permits" or "Compliance Code for Class U2/U3 Permits" as relevant.
Designated Individual(**s**)	Means individual(s) to whom the *Permit Holder's representative* delegates some of the responsibility and authority with respect to compliance with this Permit.
Director General	Means the Director General of the Australian Safeguards and Non-Proliferation Office.
Door-Facing-Door Configuration	Means the placement of shipping *TEU* container(s) adjacent to each other such that the container doors cannot be opened sufficiently to allow access into the container.
Inventory	Means the entire physical stock of *nuclear material*, irrespective of its form or usefulness, held by the Permit Holder.
Loss of control of material	Means the Permit Holder has lost the ability to apply the Permit Conditions to that material.
Manifest	Means a written summary to accompany conveyed *nuclear material* as part of the dangerous goods transport documents.
Material Control and Accountancy (**MC&A**)	Means an integrated set of measures designed to provide information on, control of, and assurance of the presence of *nuclear material*, including those systems necessary to establish and track *nuclear material* inventories, control access to and detect loss or diversion of *nuclear material*, and ensure the integrity of those systems and measures.
Nuclear Material (**NM**)	Means the same as in *the Act* but for the purposes of this Permit excludes material that has been deemed by *ASNO* as practicably irrecoverable.
Nuclear Security (as applied to *nuclear material*) or **Security**	Means the integrated set of measures intended to prevent unauthorised access to, or malicious acts against, *nuclear material* and associated infrastructure, including transport.
Permit Holder's Representative	Means the representative of the Permit Holder (i.e. the organisation) who will take responsibility and sign documents on behalf of the organisation. This person must be in a position with sufficient authority to ensure all Permit conditions are met.
Plan(**s**) (the)	Means the Permit Holder's documented plans and procedures for implementing all of the objectives and conditions of the Permit and *Compliance Codes*.
Security culture	Means the characteristics and attitudes of an organisation and individuals that establish security as a high priority, and security risks receive the attention warranted by the potential for proliferation of *nuclear material*.

SCEC and **SEEPL**	Means the Security Construction and Equipment Committee (SCEC) four level security level rating described in the Security Equipment Evaluation Product List (SEEPL)
Source Material	Means the same as in Schedule 1 of *the Act*
Subcontract	Means an arrangement entered into by the Permit Holder with a person to provide goods or services in connection with this Permit. A "Subcontractor" or "agent" has a corresponding meaning.
TEU	Means a "twenty foot equivalent unit". A measurement of shipping container capacity.
Uranium Ore Concentrate(**s**) (**UOC**)	Means Uranium oxides and other related compounds produced from and during ore processing that contain uranium greater than 50% w/v uranium.

NOTE: *Subject to the Administrative Appeals Tribunal Act 1975 and to sub-section 22(8) of the Nuclear Non-Proliferation (Safeguards) Act 1987, application may be made to the Administrative Appeals Tribunal, by or on behalf of a person whose interests are affected by a decision by the Minister, pursuant to sub-section (2) of section 13 of the Act, imposing a condition or restriction on the grant of a Permit, for review of the decision.*