

Security standards for security plans and transport security plans

Security of high consequence radioactive material

Section 16A of *Subordinate Legislation Act 1994*

Section 67N(3) of *Radiation Act 2005* – Secretary must specify security standards

Background

Section 67B of the *Radiation Act 2005* requires that the following persons must prepare and submit a security plan to an approved assessor for approval:

- a) An applicant for a management licence who intends to possess a high consequence sealed source or high consequence group of sealed sources;
- b) An applicant for a facility construction licence who intends to construct or use land for a building as a radiation facility that will house a high consequence sealed source or high consequence group of sealed sources;
- c) A management licence holder who intends to make an application to vary their management licence in order to possess a high consequence sealed source or high consequence group of sealed sources.

Section 67C of the Act requires that a security plan prepared and submitted under section 67B must –

- a) **Address the security standard specified by the Secretary under section 67N for the high consequence sealed source or high consequence group of sealed sources**; in relation to which the applicant for, or holder of, a management licence will conduct a radiation practice; and
- b) Set out the security measures to be implemented to control any issues identified in the security standard; and
- c) Include any other matters specified by the Secretary in accordance with subsection (2); and
- d) Be in the form specified by the Secretary.

Section 67N(1) of the Act states that the Secretary to the Department of Health and Human Services must specify a security standard that a security plan or transport security plan must meet to be approved by an approved assessor.

Section 67N(2) of the Act states that the security standard must set out security measures that must be met according to the level of threat from terrorist activity in relation to radiation sources.

Purpose of the document

The purpose of this document is to specify the security standards.

Minimum standards

The minimum standard of a security plan and/or transport security plan is, regardless of the source category or the threat level, that there must be:

- a) Annual review of the plan;

- b) Annual review of intrusion detection, event assessment and communication measures;
- c) Annual review of access controls and physical barriers;
- d) Annual review of staff access requirements;
- e) Annual audit of all sources;
- f) Annual staff security awareness briefing;
- g) Event specific review of staff access;
- h) Staff induction security awareness briefing;
- i) Event specific staff security awareness briefing;
- j) Monthly accounting or check to confirm presence of the source; and
- k) Visitors to be signed in and escorted while present inside the secure area defined in the security plan.

Additional security standards

The following additional standards apply depending on the security category and the prevailing security threat level as defined by the **National Terrorism Threat Level**. The National Terrorism Threat Level is published at <<https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx>>

Category 1 Sealed Sources or a Category 1 Group of Sealed Sources

When the source is in **use** or in **storage**, it must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a security guard or Police to interrupt unauthorised removal of the source.

When the source is being **transported**, it must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a security guard or Police to interrupt unauthorised access to the source.

When the security threat level is **NOT EXPECTED** or **POSSIBLE**, the source must also be protected by annual exercising of the security guard force or Police response arrangements.

When the security threat level is **PROBABLE**, the source must also be protected by taking the following additional actions:

- a) Weekly accounting or check to confirm presence of the source or sources;
- b) Annual exercising of security guard force or Police response arrangements;
- c) Half yearly review of staff access.

When the security threat level is **EXPECTED** or **CERTAIN**, the source must also be protected by taking the following additional actions:

- a) Visitors to be refused entry to the inside of the secure area as defined in the security plan, unless approved in writing by the one or more of the Department of Health and Human Services, Victoria Police, Ambulance Victoria, Metropolitan Fire Brigade or Country Fire Authority;
- b) Goods deliveries to be dispatched and received off-site with movement of goods only to be undertaken by persons whose identity has been verified by the management licence holder;
- c) Half yearly staff security awareness briefing;
- d) Daily accounting or check to confirm presence of the source or sources;
- e) Annual exercising of security guard force or Police response arrangements;

- f) Half yearly review of staff access.

Category 2 Sealed Sources or a Category 2 Group of Sealed Sources

When the source is in **use, in storage or being transported**, it must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source.

When the security threat level is **PROBABLE**, the source must also be protected by taking the following additional actions:

- a) Weekly accounting or check to confirm presence of the source or sources;
- b) Annual exercising of security guard force or Police response arrangements;
- c) Half yearly review of staff access.

When the security threat level is **EXPECTED** or **CERTAIN**, the source must also be protected by taking the following additional actions:

- a) Visitors to be refused entry to the inside of the secure area as defined in the security plan, unless approved in writing by one or more of the Department of Health and Human Services, Victoria Police, Metropolitan Fire Brigade or Country Fire Authority;
- b) Goods deliveries to be dispatched and received off-site with movement of goods only to be undertaken by persons whose identity has been verified by the management licence holder;
- c) Half yearly staff security awareness briefing;
- d) Daily accounting or check to confirm presence of the source or sources;
- e) Annual exercising of security guard force or Police response arrangements;
- f) Half yearly review of staff access.

Category 3 Sealed Sources or a Category 3 Group of Sealed Sources

When the source is in **use, in storage or being transported**, it must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force.

When the security threat level is **PROBABLE**, the source must also be protected by taking the following additional actions:

- a) Weekly accounting or check to confirm presence of the source or sources.

When the security threat level is **EXPECTED** or **CERTAIN**, the source must also be protected by taking the following additional actions:

- a) Visitors to be refused entry to the inside of the secure area as defined in the security plan, unless approved in writing by one or more of the Department of Health and Human Services, Victoria Police, Metropolitan Fire Brigade or Country Fire Authority;
- b) Goods deliveries to be dispatched and received off-site with movement of goods only to be undertaken by persons whose identity has been verified by the management licence holder;
- c) Half yearly staff security awareness briefing;
- d) Daily accounting or check to confirm presence of the source or sources;
- e) Annual exercising of security guard force or Police response arrangements;
- f) Half yearly review of staff access.