INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

Mission Report: Australia

04-15 November 2013

Prepared for the Australian Government

Distribution of this IPPAS mission report is at the discretion of the Australian Government. The IAEA will make the report available to third parties only with the express permission of the Australian Government. Any use of or reference to this report that may be made by the competent agencies is the responsibility solely of the agency in question.

ABBREVIATIONS

AACS	Automated Access Control System
ADS	Accreditation Document Set
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASNO	Australian Safeguards and Non-Proliferation Office
BYOD	bring your own device
CAS	central alarm station
CCTV	Closed Circuit Television
CPPNM	*Convention on the Physical Protection of Nuclear Material* (INFCIRC/274/Rev.1)
DBT	design basis threat
FPS	Frames per second
HEU	highly enriched uranium
I&C	Instrumentation and Control
NSS 13	Information Circular 225/Revision 5 (Corrected), *Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities*
IPPAS	International Physical Protection Advisory Service
IRAP	Information Security Registered Assessors Program
ISM	Information Security Manual
ITSA	Information Technology Security Adviser
LEU	low enriched uranium
MA&C	material accounting and control
MAC	Mandatory Access Control
NM	nuclear material
NPP	nuclear power plant
NSS	IAEA Nuclear Security Series
PAB	Panic Actuator Button
PIDS	Perimeter Intrusion Detection System
PSPF	Protective Security Policy Framework
RCMS	Reactor Control Management System
RM	radioactive material
RPS	Radiation Protection Series

SCC	Site Control Centre
SCEC	Security Construction Equipment Committee
SyOPs	Security Operation Procedures

CONTENTS

SUMMARY

The International Physical Protection Advisory Service (IPPAS) team, following a formal request from the Australian Government, conducted a nuclear and cyber security review at the Commonwealth-level and specifically at a nuclear facility during the period 04-15 November 2013. The IPPAS team was composed of international experts in physical protection, guards and response forces, a legal expert, and cyber security expert.

The IPPAS team met with officers from the competent authorities, the Australian Safeguards and Non-Proliferation Office (ASNO) and the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). The team found that there was a comprehensive coverage in Commonwealth legislation for the obligation of the State to establish, implement, and maintain a physical protection regime as recommended by the International Atomic Energy Agency (IAEA) in its publications, *Nuclear Security Recommendation on Physical Protection of Nuclear Material and Nuclear Facilities* (NSS 13) and *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* (NSS 14).

The IPPAS team visited the Australian Nuclear Science and Technology Organisation (ANSTO) to review the implementation of physical protection regulation, transport and cyber security. The nuclear security procedures and measures in use were presented, explained and discussed.

The IPPAS team were impressed with the Australian Government's awareness of the importance of physical protection and their commitment to its further improvement. The cooperation at both the Australian Government and facility levels enabled the team to gain a good understanding and appreciation of the current status of the relevant national legislation and of the physical protection, including cyber protection, of nuclear and radioactive material and associated nuclear facilities.

Australian Government (Commonwealth) level

Only the Commonwealth level was reviewed during this mission.

Good cooperation was evident between competent authorities.

There are many authorities that have roles for the security of nuclear and other radioactive material, associated activities and facilities; the various requirements are not fully harmonized and not collected within a single requirement document.

General security awareness of the government authorities is very high.

A high priority is assigned to security issues, which help sustain the level of security of Australian Government organizations.

General security standards are shared across the whole government sector.

No regulations for the security of nuclear material have been promulgated.

There are no established security requirements for unsealed sources and radioactive waste.

The Australian Government should introduce a requirement for a regular review and update of the physical protection regime.

Facility level

The ANSTO facility at Lucas Heights was the only site visited by the IPPAS team. All nuclear material and other radioactive material, associated activities and facilities, as well as user level security measures reviewed in the report are on its single site.

Physical protection arrangements are changing, since category I nuclear material has been totally removed and the site is now a category II facility– many legacy of the former physical protection arrangements (currently not required) are still left/available on-site.

Full review of all security related documents was requested in a joint letter by the CEO of ARPANSA and the DG of ASNO.

An active review process of security documentation was evident with many documents recently updated. However, these had not yet been seen by the regulator.

General state of physical protection equipment is very good reflecting the support from ANSTO management.

Very comprehensive security management procedures were observed. However, there is a lack of overarching integration as per NSS 13 and 14, as many different requirements are reflected in many different documents.

Protection in depth principle is generally well applied. However, in some cases, the protection was seen to be unbalanced (certain routes are much better protected than others).

Well developed employee trustworthiness check programme is applied.

Strong security culture programme is established and maintained.

I. INTRODUCTION

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) conducted for the Australian Government during 04-15 November, 2013.

Since its inception in 1995, the purpose of IPPAS has been to provide advice and assistance to strengthen the effectiveness of State systems of physical protection of nuclear material and facilities. This scope of IPPAS missions was later extended to provide also advice and assistance in the field of security of radioactive materials.

A formal request from the Australian Government to conduct an IPPAS mission was received by the IAEA on 21 November 2011. The IAEA agreed to conduct the IPPAS mission to Australia in November 2013. The initial meeting was held in September 2012, in the margins of the General Conference 56 meetings in Vienna during which the general issues related to the conduct of the mission were discussed. The Office of Nuclear Security (ONS), jointly with the Australian Safeguards and Non-Proliferation Office (ASNO) and the Australian Nuclear Science and Technology Organisation (ANSTO) conducted a Regional Workshop on the IPPAS from 5 - 7 November 2012 in Sydney. The IPPAS preparatory meeting was held on 8 - 9 November 2012 in Sydney.

The objectives of the mission were to:

> Make an assessment of the Australian nuclear security regime and its implementation, and to compare the procedures and practices in Australia with the CPPNM and its 2005 Amendment, the IAEA *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (*INFCIRC/225, Rev. 5,)* referred to hereinafter simply as *NSS 13*, and other Nuclear Security Series (NSS) guidance documents;

The scope of the mission was to:

> Review the Australian nuclear security legislative and regulatory framework for nuclear and other radioactive material and associated facilities, regulatory practices (licensing, inspections and enforcement) and coordination between organisations involved in physical protection on Commonwealth level. The conduct of the mission covered a review and evaluation of the physical protection systems in place at ANSTO, as well as the assessments of the physical protection arrangements for transport of nuclear and other radioactive material to and from ANSTO and cyber security. The interface with the nuclear material and accountancy procedures were addressed during the mission.

The IPPAS mission team (see Appendix II) consisted of international experts in physical protection, a legal expert, a cyber-security expert and an IAEA technical officer.

The team gathered information on the legal and regulatory structure on Commonwealth level through interviews with senior management personnel from ASNO, ARPANSA, ANSTO, the Australian Federal Police (AFP), the ASIO T4 Protective Security section, the Attorney-General's Department and the Australian Signals Directorate (ASD). Also, visits were made to the Australia's Open Pool Australian Light-water (OPAL) Reactor and different buildings at the ANSTO facility at Lucas Heights, Sydney. The team observed the implementation of physical protection practices and held discussions with facility personnel. The meetings and the facility visits also provided a forum for an

informal exchange of information on physical protection practices used in other countries and the opportunity to discuss the technical aspects of implementing physical protection systems.

During the review, the team experienced outstanding cooperation from the host country personnel at all technical and management levels. All participants were enthusiastic and interested in obtaining international experience and advice on the best way to conduct their work and perform their duties. Their willingness to discuss sensitive issues was appreciated as the team members were aware of the need to exercise discretion with regard to all mission-related information. The information contained in this report will be protected in accordance with IAEA guidelines for Highly Confidential information.

NATIONAL LEVEL REVIEW

II. GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES AND INTERNATIONAL OBLIGATIONS

The Australian Government (also referred to as Federal Government and the Commonwealth Government) is subject to the Australian Constitution, a legislator for all of Australia. Certain responsibilities and powers are divided between the Federal Parliament and state or territory parliaments. If a state/territory law conflicts with a federal law, in accordance with section 109 of the Constitution the federal law prevails over the state/territory law to the extent of the inconsistency. Section 122 of the Constitution allows the Federal Parliament to override a territory law.

The Australian Government (also referred to as Federal Government, Commonwealth Government) is a legislator for the whole country. Section 51 of the Constitution defines issues that the Australian Government can make laws on. If Commonwealth legislation is required to give effect to a treaty, the Government relies on the external affairs power in Section 51 (xxix) of the Constitution.

Nuclear security is governed primarily by the *Nuclear Non-Proliferation (Safeguards) Act 1987* (the Safeguards Act), providing legislative basis for ASNO's activities related to, inter alia, safeguards and security of nuclear material and items. ASNO is in this respect the main nuclear security regulatory body in Australia, complemented by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). However, some roles belong to (or are shared with) other bodies, having roles in performing tasks specific for their position within government.

Accordingly, the regulatory nuclear security regime in Australia primarily involves ASNO as the regulator for nuclear material. ARPANSA has responsibilities, inter alia, for radiation protection, nuclear safety and security of radioactive material. It maintains the National Sealed Source Register (NSSR) database and acts as the National Competent Authority both domestic and abroad for Emergency Preparedness and Response under the Conventions for Early Notification and Assistance. It is of important to note that ARPANSA, unlike ASNO, exercises its powers directly only in relation to controlled persons who are essentially Commonwealth entities, their contractors and their authorised employees.

Since ASNO and ARPANSA share to some extent responsibilities for nuclear security regulation, they regularly communicate regarding nuclear security and other related regulatory matters. To this end they signed a Note of Understanding in 2001 "concerning evaluation of physical protection and security arrangements for the Replacement Research Reactor at Lucas Heights and the protection of associated information." In that Note, it was agreed that the two organisations shared the responsibility for evaluation of the physical protection and security arrangements for OPAL and that each had their specific domains of expertise. Acceptance criteria for the security plan for the OPAL facility were then developed and jointly agreed. Furthermore, in Section 4.5 of the ARPANSA Chief Executive Officer's (ARPANSA CEO) "Statement of Reasons" regarding the decision on application by ANSTO for a licence to operate the OPAL reactor sets out how ASNO and ARPANSA cooperated regarding the licencing process for the OPAL reactor.

In 2006, ASNO and ARPANSA established a new Memorandum of Understanding (MoU) for the co-operation and exchange of information in nuclear regulatory matters. The MoU was revised on 17 February 2012. In 2011, ARPANSA and ASNO established a Physical Protection and Security Working Group for the purpose of conducting a security review of OPAL in accordance with CEO ARPANSA's Statement of Reasons mentioned above. The same working group is considering security

arrangements for current building projects at ANSTO. As stated in the Notification letter by ARPANSA CEO and ASNO Director General (ASNO DG) addressed to ANSTO, "this arrangement will simplify the reporting process, allowing ANSTO to provide information to both regulators simultaneously, reducing the workload and preventing the duplications of tasks and activities".

The power to enter into treaties is an executive power within Section 61 of the Australian Constitution. Decisions about the negotiation of multilateral conventions, including determination of objectives, negotiating positions, the parameters within which the Australian delegation can operate, and the final decision as to whether to sign and ratify can be taken at Ministerial level, however in most cases is taken by Cabinet.

Australia is a party to all relevant international agreements related to nuclear field covering the areas of nuclear security, non-proliferation, emergency preparedness, waste management and nuclear safety.

Australia is a party to the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment (Ratified 22/09/1987 and 17/07/2008), International Convention for the Suppression of Acts of Nuclear Terrorism (ratified 16/03/2012). It submitted (approved) reports on UNSCR 1540 Committee Approved Matrix, UNSCR 1540 (S/AC.44/2004/(02)/53) and UNSCR 1540 (S/AC.44/2004/(02)/53/Add.1). Australia is a founding member the Global Initiative to Combat Nuclear Terrorism (GICNT) and has participated in Global Partnership and Proliferation Security Initiative. INFCIRC/225/Rev.5 (NSS 13) is a licence requirement for all nuclear facilities.

Australia supports the Code of Conduct on the Safety and Security of Radioactive Sources (confirmed through political commitment pursuant to GC(47)/RES/7), Supplementary Guidance on the Import and Export of Radioactive Sources (confirmed through political commitment pursuant to GC(48)/RES/10) and keeps National sealed sources register for Category 1 and 2 sources. Australia hosted Integrated Regulatory Review Service (IRRS) missions in 2007 and 2011. Australia participates actively in international working groups focused on nuclear forensics and detection (GICNT Nuclear Forensics Working group, GICNT Response and Mitigation Working Group, GICNT Nuclear Detection Working Group, Nuclear Forensics International Technical Working Group). Australia's major involvement in IAEA activities comprises membership in Advisory Group on Nuclear Security (AdSec), Nuclear Security Guidance Committee (NSGC) and Emergency Preparedness and Response Expert Group, IAEA Radioactive Source Security Working Group, Incident & Trafficking Database and Analytical Laboratories for the Measurement of Environmental RadioActivity (ALMERA).

Australia also participates in the IAEA Coordinated Research Project on Identification of High Confidence Nuclear Forensic Signatures for the Development of Nuclear Forensic Libraries, it chairs experts group on information exchange for Code of Conduct on the Safety and Security of Radioactive Sources, provides expert consultant for Development and review of Nuclear Security Series documents, provides expert consultants and presenters for regional IAEA Nuclear Security Training Courses and other courses led by IAEA Office of Nuclear Security. Team members are provided for International Physical Protection Advisory Service (IPPAS) Missions. Australia contributes to the IAEA Nuclear Security Fund.

Among other outreach and capacity building events, Australia has recently hosted or organised IAEA regional workshop on the nuclear security in the transport of nuclear material (2012), IAEA regional workshop on IPPAS missions (2012), IAEA Regional Workshop on Radiological Crime Scene Management and Introduction to Nuclear Forensics (2012), IAEA regional training courses on nuclear forensics and radiological crime scene management (2008 – present). IAEA regional training courses on nuclear security of research facilities were held in Australia (2004, 2006, 2009).

ASNO is currently registered with the IAEA as the point of contact for the CPPNM. The obligations stemming from CPPNM are ensured by the Safeguards Act.

Good practice 1:

Australia, in addition to being involved in all relevant international nuclear security legal (or soft-law) instruments, plays a leading role in a number of international and regional outreach activities aimed at strengthening international nuclear security regime, whereby it intensely exchanges information both directly and through the IAEA and other relevant international organisations.

It was established that at instances where there are more governmental entities involved in regulation of nuclear security, the responsibilities are almost always well coordinated among these entities, such as when ASNO and ARPANSA develop common policy in terms of nuclear security requirements through memoranda of understanding and maintaining Physical Protection and Security Working Group. However, it would be beneficial to approach the nuclear security regime with a clearer assignment of responsibilities to reduce the potential for duplication or inconsistent approaches.

There is no in-built procedure to review and update regularly Australia's physical protection regime as required by NSS 13. In practice, the review and update is carried out on as-needed basis.

Basis:

NSS13 paragraph 3.2 - The State's *physical protection regime* should be reviewed and updated regularly to reflect changes in the *threat* and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of *nuclear material* and *nuclear facilities*.

Recommendation 1:

The Australian Government should introduce a requirement for a regular review and update of the physical protection regime.

III. NATIONAL PHYSICAL PROTECTION REGIME

III.1. Laws

There are two main Commonwealth Acts that provide for the protection of nuclear and other radioactive material and facilities, the *Nuclear Non-Proliferation (Safeguards) Act 1987* (hereinafter "Safeguards Act") and *The Australian Radiation Protection and Nuclear Safety Act 1998* (hereinafter "ARPANS Act").

The Australian physical protection regime is established by the Safeguards Act that expressly addresses CPPNM by defining as one of its objects giving effect to certain obligations that Australia has as a party to CPPNM (annexed as Schedule 4 of the Act).

By Administrative Orders, the Safeguards Act is administered by the Minister for Foreign Affairs through ASNO and the ARPANS Act by the Minister for Health.

Licencing authorities involved in nuclear security in Australia hence are ASNO and ARPANSA.

The Safeguards Act has been in effect since 31 March 1987. It implements Australia's obligations under the NPT, Australia's safeguards agreement and Additional Protocol with the IAEA, agreements between Australia and various countries (and Euratom) concerning transfers of nuclear items and cooperation in peaceful uses of nuclear energy, the Convention on the Physical Protection of Nuclear Material and its 2005 amendment and the International Convention for the Suppression of Nuclear Terrorism.

It establishes a system for control over nuclear material and associated items in Australia through requirements for permits for, inter alia, their possession and transport.

The Safeguards Act provides ASNO with the authority to ensure the effective operation of the Australian safeguards system and ensure the physical protection and security of nuclear material and items in Australia.

Recent major revisions of the Safeguards Act include the *Non-Proliferation Legislation Amendment Act 2003*, which strengthened arrangements and offences for the protection and safeguards of nuclear material, facilities and associated information and introduced a permit requirement for the establishment of any new nuclear facility in Australia. Furthermore, the *Non-Proliferation Legislation Amendment Act 2007* gave legal effect to Australia's obligations under the amended CPPNM, introduced a permit requirement for the decommissioning of nuclear facilities and extended the geographical jurisdiction for some offences. Finally, the *Nuclear Terrorism Legislation Amendment Act 2012* introduced Additional Offences required for the ratification of International Convention on the Suppression of Act of Nuclear Terrorism.

Section 3(1) of the Safeguards Act states the principal object, which is to give effect to, inter alia, certain obligations that Australia has as a party to the prescribed international agreements. That includes Australia's network of Nuclear Cooperation Agreements which specify that nuclear material subject to these agreements shall be protected according to NSS 13 (of various revisions).

Section 3(3) of the Safeguards Act states that further object is also to give effect to certain obligations that Australia has as a party to the International Convention on the Suppression of Act of Nuclear Terrorism.

As a prerequisite for obtaining a permit based on the Safeguards Act it is stipulated in section 13(3) thereof that the Minister (or his delegate) may grant permits for the possession of nuclear material subject to restrictions and conditions in respect of, inter alia, "the measures to be taken to ensure the physical security of nuclear material" and "the taking of measures that are consistent with Australia's obligations under the Physical Protection Convention". Similar provisions specifying security

conditions in permits cover transport of nuclear material (section16), establishing a nuclear facility (section 16A) and decommissioning (section 16B). According to section 19 the Minister may revoke a permit if the holder of the permit

- contravenes a condition, or fails to observe a restriction, subject to which the permit or authority is granted
- contravenes a direction given or an order made under section 73; or
- is convicted of an offence against the Safeguards Act.

Inspections are covered by Divisions 3 and 4 of Part IV of the Safeguards Act. It provides for appointment of inspectors by the Minister (this has been delegated to Director General ASNO), roles and powers of inspectors including entry into land, premises, vehicle or vessel occupied by the permit holder (section 59). Provisions on search, warrants and seizures are covered by sections 61-64. The information inspectors may require is specified in section 66. General information regarding the outcomes of ASNO inspections are reported to parliament annually.

Offences are covered by Part III of the Safeguards Act, they include, for example.

- breach of duty to ensure security of associated technology,
- communication prejudicing security of nuclear material or associated item,
- unauthorized access to areas etc. to which access is restricted under permit

Offences relating to the CPPNM are expressly covered by Division 2 of Part III of the Act. In compliance with amended CPPNM, they include:

- stealing nuclear material,
- demanding nuclear material by threats etc.,
- unauthorised carrying, sending or moving nuclear material,
- use of nuclear material causing death or injury to persons or damage to property or the environment,
- acts against nuclear facilities, threat to use nuclear material, threat to commit offence.

Division 2A covers offences relating to nuclear terrorism, inter alia:

- possessing specified radioactive material or device, or making such device to cause the death or serious bodily injury or substantial damage to property or to the environment
- using radioactive material, or using or damaging specified device or nuclear facility to cause the death, serious bodily injury or to cause substantial damage to property or to the environment; or to compel a person or group of persons to do or refrain from doing any act or thing,
- pertinent threats and demands.

No administrative offences have been established by the Safeguards Act.

As stipulated by Section 7 thereof, nothing therein renders the Crown liable to be prosecuted for an offence.

The other primary piece of legislation dealing with nuclear security aspects, the ARPANS Act focuses primarily on radiation protection. As stipulated in its Section 3, the object of the ARPANS Act is to

protect the health and safety of people, and to protect the environment, from the harmful effects of radiation. The ARPANS Act is applicable to 'controlled persons', defined in section 13 of the Act. The definition restricts 'controlled persons' to Commonwealth entities and Commonwealth contractors and their employees. 'Controlled persons' do not include persons or organisations that are licensed or regulated by State or Territory governments. Under sections 32 and 33 the CEO of ARPANSA may issue a facility or source licence to a controlled person, taking into account international best practice in relation to radiation protection and nuclear safety and the matters prescribed in the Regulations. The licence may, according to section 35, contain conditions, both at the time of issuing the licence and after the licence is issued, which can include security requirements.

Section 9 of the ARPANS Act provides that the Safeguards Act is capable of operating concurrently with the ARPANS Act. That means in practice that a controlled person may be required by the ARPANS Act to hold a licence, and by the Safeguards Act to hold a permit, in respect of the same thing. The controlled person must satisfy the requirements of both Acts.

The ARPANS Act prohibits certain conduct in relation to controlled facilities (nuclear installations and prescribed radiation facilities) or dealings with controlled material or apparatus unless authorised by a facility or source licence or unless the conduct or dealing is exempted by the Regulations (sections 30 and 31).

Non-compliance with a licence condition is an offence under subsections 30(2) and 31(2) of the ARPANS Act. Non-compliance with a licence condition could also result in the CEO suspending or cancelling a licence (section 38), imposing additional licence conditions or reducing the authority granted by a licence (section 36) or issuing a formal direction to a licence holder to take certain steps (section 41), the non-compliance of which may result in the suspension or cancellation of the licence.

Trustworthiness of persons is not expressly addressed either in nuclear-related laws or regulations. In practice, ensuring vetting procedures of persons and confidentiality of documents is one of the conditions attached to a pertinent permit or licence, whereby the regulated entities are usually obliged to follow core principles identified in the Australian Government Protective Security Policy Framework (PSPF).

No administrative offences relating to financial penalties, such as administrative fines for noncompliance have been established by the ARPANS Act.

According to section 4 of the ARPANS Act, nothing therein renders the Crown liable to be prosecuted for an offence.

As mentioned above, the main regulated entity, ANSTO (or any other Commonwealth entity), cannot be prosecuted, neither based on the Safeguards Act, nor the ARPANS Act, should a situation demanding such a procedure occur.

Basis:

NSS13 paragraph 3.15 - Enforcement of physical protection regulations should be a part of a State's legislative and regulatory framework.

Recommendation 2:

The Australian Government should review its legislation to ensure that there are no situations where an offender is exempt from sanctions. The review should also bear in mind the absence of administrative offences for less serious breaches of the legislative requirements.

The team did not observe a specific provision which places "prime responsibility" for security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets. The team thinks it would be beneficial for legislation to expressly allocate prime responsibility to the authorized persons.

The IPPAS team was advised that nationally, in accordance with the ANSTO Act Section 5(bc), there is a mechanism for a designated entity to assume prime responsibility for security in the absence

of "authorized persons". Of note, while ARPANSA and ASNO have the right of seizure of material as inspectors, there was no evidence of a documented procedure to assure "control" of the seized or orphaned material (eg. enabling mechanism(s) or link(s) between ARPANSA/ASNO and ANSTO).

Suggestion 1:

All relevant Australian authorities should complete enabling mechanisms to formalize the process for a designated entity to assume prime responsibility for security in the absence of "authorized persons".

III.2. Secondary Legislation

Implementing secondary legislation with respect to the Safeguards Act can be issued in accordance with Section 74(f) thereof as "standards for the physical security to be applied with respect to nuclear material and associated items…". The current Nuclear Non-Proliferation (Safeguards) Regulations 1987 do not specify any security standards. In practice, these are specified in permits granted pursuant to the Safeguards Act. Various national guidelines and also NSS 13 is referred to in permits as a requirement for all nuclear facilities.

According to section 73 of the Safeguards Act the Minister may, by legislative instrument, make orders, not inconsistent with the Safeguards Act or the regulations, to be complied with by the holders of permits. The Minister may also give directions to be complied with by the holder of a permit. However, as established based on the information from ASNO, no orders or directions have been made with respect to the security of nuclear material as yet.

Under section 85 of the ARPANS Act the Governor General may make regulations on certain matters.

Among the matters prescribed in ARPANS Regulations 41 and 42, is a requirement for the CEO to take into account if the information provided by an application establishes that the proposed conduct or dealing can be carried out without undue risk to the health and safety of people, and to the environment.

Regulation 39 of the Regulations also provides that the CEO may request information from licence applicants. This could either be information in Part 1 (facility licence) or Part 2 (source licence) of Schedule 3 to the Regulations or any other information that is appropriate to the licence application. The information that the CEO may request includes information on the security plan and information on the emergency plan for the controlled facility, apparatus or material.

All the information that the CEO may request under Part 1 and Part 2 of Schedule 3 to the Regulations have been included in guidelines issued by the CEO to potential licence applicants. Under Regulation 48 of the ARPANS Regulations it is a condition of a source or facility licence that all conduct and dealings with controlled material, controlled apparatus and controlled facilities are in accordance with the Code of Practice for the Security of Radioactive Sources (2007, ARPANSA Radiation Protection Series No. 11).

Regulation 50 of the ARPANS Regulations stipulates that it is a condition of a source or facility licence that the holder of a license must, at least once every 12 months, review and update any plans and arrangements for managing the controlled facility, controlled material or controlled apparatus to ensure the health and safety of people and protection of the environment (under Schedule 3 to the Regulations, plans and arrangements of a licence holder must include security and emergency plans).

The applicability of ARPANSA Codes and Standards is considered by the Regulatory Assessment Report (RAR) as being a part of the advice provided by regulatory officers reviewing an application for a particular licence - the CEO takes such information into account. Code of Practice for the Security of Radioactive Sources is of particular relevance. This particular code can be applied to

facilities, sources and any dealings, including storage, use, disposal and transportation. Licence applicants are required to demonstrate compliance with RPS-11 in order to gain and maintain a licence.

There are numerous Radiation Protection Series (RPS) documents and many contain security requirements specific to the particular dealing, facility or apparatus. RPS 11 provides the fundamental requirements for the security of radioactive sources. All RPS documents are incorporated by reference in the National Directory of Radiation Protection in cooperation with all States and Territories. Once a RPS document is incorporated by reference into the National Directory, every Australian jurisdiction must adopt it as law in its jurisdiction, which is how national uniformity in radiation protection and nuclear safety is promoted by ARPANSA.

Nuclear security related requirements based on the ARPANS Act are directly binding only for Commonwealth entities, which could potentially lead to different treatment of licensed activities (facilities) of the same kind subject to different jurisdictions; however, procedures to ensure uniformity were noted by the IPPAS team.

Suggestion 2:

The Australian Government should consider making a formalised arrangement specifying pertinent requirements applicable across the country that would ensure clearer uniformity and predictability of regulation.

Nuclear security related requirements covered by the Safeguards Act are based on customized permit conditions.

Basis:

NSS20 paragraph 3.3(e) – The legislative and regulatory framework, to govern the nuclear security regime … provide for the establishment of nuclear security regulations and requirements.

NSS13 paragraph 3.11 - The State's legislation should provide for the comprehensive regulation of physical protection and include a licensing requirement or other procedures to grant authorization. The State should promulgate and review its regulations for the physical protection of *nuclear material* and *nuclear facilities* regularly.

Recommendation 3:

The Australian Government should promulgate nuclear security requirements in regulations.

IV/A. ROLE & RESPONSIBILITIES OF COMPETENT AUTHORITY - ASNO

IV/A 1 Authority, Resources and Independence

In accordance with the *Nuclear Non-Proliferation (Safeguards) Act 1987*, Australian Safeguards and Non-Proliferation Office (ASNO) is led by a Director appointed by the Governor-General and reports to the Minister of Foreign Affairs at the ministerial level of the Government.

In accordance with Section 43 of the Act, the Director is responsible for the following functions:

a) to ensure the effective operation of the Australian safeguards system;

b) to carry out, on behalf of Australia, the obligations that Australia has under the Agency Agreement, the Supplementary Agency Agreements and the prescribed international agreements to report in relation to the operation of the Australian safeguards system;

c) to monitor compliance with the provisions of the prescribed international agreements by parties other than Australia;

d) to undertake, co-ordinate and facilitate research and development in relation to nuclear safeguards;

e) to advise the Minister on matters relating to the operation of the Australian safeguards system;

f) to carry out such duties, and to exercise such powers, as are conferred on the Director by or under this Act or the regulations or any other law of the Commonwealth; and

g) to do anything incidental or conducive to the performance of any of the functions referred to in the preceding paragraphs.

The IPPASs team was informed that the Competent Authority has the adequate financial, competence and human resources to meet its functional assignments.

The Competent Authority has the capacity to seek contractual staff augmentation if needed and may seek additional expertise from other Commonwealth organizations such as Australian Radiation Protection and Nuclear Safety Agency and other Government Departments and agencies to assist in the fulfilment of its duties. This was evident through its practice of co-reviewing and assessing Australian Nuclear Science and Technology Organization (ANSTO) applications for licencing the OPAL reactor along with Australian Radiation Protection and Nuclear Safety Agency.

ASNO is the mandated organization to fulfil the following roles:

- regulation of the security of nuclear material and facilities and associated items (material, equipment and technology)
- engagement with state and federal government agencies
- assisting the development of nuclear security standards internationally
- training and outreach
- other international engagement (e.g. Nuclear Security Summit)
- Australia's designated point-of-contact for the CPPNM
- Australia point-of-contact for the IAEA ITDB in relation to nuclear material

In spite of the information provided that sufficient human resources were assigned to the competent authority for security, it was noted through the course of the mission, that there were critical submissions from the permit holder (periodic security review) that were not receiving timely review and approval. There are a total of two staff assigned duties for regulating nuclear security and their section covers broad areas of responsibility. In the event of a singular absence from the workplace, the responsibilities fall to one person, leaving no resiliency. It was also observed that there is no "surge capability" to respond to unforeseen circumstances.

Suggestion 3:

It is suggested that the staffing level of the regulator be examined to determine the appropriateness of the current staffing level for security responsibilities.

The competent authority carries out its functions independent of the operators or permit holders in ensuring that physical protection measures are being met by the permit holders. The competent authority is provided information regarding the threats against nuclear material, including the national threat assessment from Commonwealth organizations and uses this information in the development of the Design Basis Threat. A design basis threat is developed by the regulatory body for application by ANSTO. The effectiveness of these measures are assessed against the threat.

The regulatory body has not defined the unacceptable radiological consequences (URC) and still requires protection against sabotage. A graded approach is being applied however without a defined value for the URC

Basis:

NSS13 paragraph 3.43 - A *graded approach* is used to provide higher levels of protection against events that could result in higher consequences. The State should decide what level of risk is acceptable and what level of protection against the threat should be provided.

NSS13 paragraph 3.44 - For protection against *unauthorized removal*, the State should regulate the categorization of *nuclear material* in order to ensure an appropriate relationship between the *nuclear material* of concern and the *physical protection measures*. For protection against *sabotage*, the State should establish its threshold(s) of *unacceptable radiological consequences* in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection.

Recommendation 4:

The Australian Government should define the URC or provide formal guidance on the bounding conditions that should be used to determine adequacy of protection to potential sabotage targets.

Suggestion 4:

The Australian Government should consider defining a procedure for establishing the level for high radiological consequences as per NSS 13.

The team was not provided evidence that a regulatory body had established a national detection strategy including for effective detection at its borders for the detection of nuclear or other radioactive material entering or leaving the border.

Basis:

The legislative and regulatory framework should:

NSS20 paragraph 3.3(c) - establish measures to ensure proper coordination and communication among *competent authorities*, and between *competent authorities* and *authorized persons*, in fulfilling their nuclear security responsibilities.

NSS20 paragraph 3.3(j) - establish law enforcement systems and measures relevant to nuclear security. These systems and measures should include those for the export, import, and for border control of *nuclear material* and *other radioactive material*. This includes security procedures for transport that are consistent with the responsibilities as set forth in Essential Element 4 when international transport is involved.

NSS20 paragraph 3.3(k) - take appropriate and effective steps to prevent, deter, detect, respond to, and otherwise combat illicit trafficking in *nuclear material* and *other radioactive material*.

Recommendation 5:

The Australian Government should extend national plans for locating, recovering and assuming control of material out of regulatory control at the border. Further it should define the roles and responsibilities of appropriate state response organizations to locate and recover any missing or stolen material.

It was determined through discussions and reviews of documents that the state has effective processes for import and export controls.

IV/A 2 Regulatory Guides

The Regulatory body (ANSO) is enabled through the Act to produce regulations. Section 74(f) of the Act provides for regulations to prescribe matters with respect to "standards for the physical security to be applied with respect to nuclear material".

The Regulatory body has not produced guides in the area of security requirements. The Regulatory body makes extensive use of existing documents, Standards and Guides developed by and for the use of Commonwealth departments and agencies. The documents, standards and guides produced for the whole of Government, enable a uniform structure and alignment to approaches, requirements and compliance across its departments and agencies. These documents become binding on the operator(s) though reference in licence condition(s). Through reference in permit conditions, ASNO can and does apply the Australian Government's Protective Security Policy Framework and its associated standards and guidance to its permit holders. This methodology was demonstrated and being effective as it applies to the ANTSO facilities.

IV/A 3 Licensing/Authorization Process

According to Articles 13 and 16 of the Act, Australia has a licensing/authorization process for nuclear activities concerning:

a) Permit to Establish a Facility (Section 16A)

b) Permit to Decommission a Facility (Section 16B)

c) Permit to Possess Nuclear Material or Associated Items (Section 13)

d) Permit to Transport Nuclear Material or Associated Items (Section 16) (May be included in Permit to Possess Nuclear Material or Associated Items through permit condition) and

e) Authority to Communicate Information (Section 18)

Further, Section 73 of the Act enables for issuance of Orders and Directions to be complied with by permit holders. It was noted through information provided, that no orders or directions had been made with respect to the security of nuclear material.

ASNO issues permits when the conditions of the permits are fulfilled. It was determined through discussions and review of an issued permit that "regulatory hold points" (i.e.; no off site transportation of Category I or II nuclear material may be made until the Competent Authority has reviewed and approved the transportation security plan for the specific transport activity) are applied within condition of permits to ensure obligations of the permit holder are met as/when required in the case of a broad permit.

ASNO utilizes permit conditions as the communicative tool to provide the minimum requirements respecting the security of nuclear materials and associated facilities in use, storage and transport. In the case of the permit issued to Australian Nuclear Science and Technology Organisation (ANSTO),

the security conditions include specified requirements in the following broad areas of Physical Protection and Information Security:

- Security Management
- Site Security and Threat Assessments
- System of Physical Protection and Security
- Access Control
- Personnel Security
- Security of Information Management (IM) Systems
- Transport Security
- Performance Assessment/testing
- Record Keeping Reporting and
- Security Program Review

The IPPAS team noted that these permits are not publically available from the Competent Authority.

IV/A 4 Inspection and Enforcement

While compliance is the responsibility of the permit holder, ASNO recognises its responsibility to communicate clearly what behaviour and performance are required to demonstrate compliance. ASNO encourages permit holders (and applicants) to implement effective company internal compliance policies to avoid situations of non-compliance or the inadvertent commission of an offense under legislation.

ASNO plans and executes a monitoring strategy informed by risk (i.e. scaled or proportionate) to achieve compliance goals. Monitoring includes such activities as monitoring performance, inspecting, analysing reports, reviewing exercise outcomes including performance testing exercises and investigating alleged/possible incidents of non-compliance.

It was determined through document review and discussions that ASNO has trained and qualified inspectors.

It was determined through the course of discussions and presentations that inspections are planned and set based on the budgetary cycle and typically are conducted at the following frequency;

- 1-2 per year at ANSTO
- every uranium mine each 12-18 months
- occasional transport
- Small permits holders infrequently

Further, it was determined through document review and discussions that, as applies to ANSTO, ASNO has established protocols with ARPANSA for the coordinated reviews of plans etc. as are appropriate and where cross cutting issues exist. This minimizes the potential for different regulatory body messaging or inconsistent/conflicting application of requirements.

Currently, it encourages ongoing compliance or return to compliance and has the authority to provide Directions or orders, the authority to restrict or revoke permits and to seek to apply sanctions as provided in the Act.

Corrective action is most commonly required through directions from the Director-General and also through required actions stipulated in inspection reports.

IV/B. ROLE & RESPONSIBILITIES OF COMPETENT AUTHORITY - ARPANSA

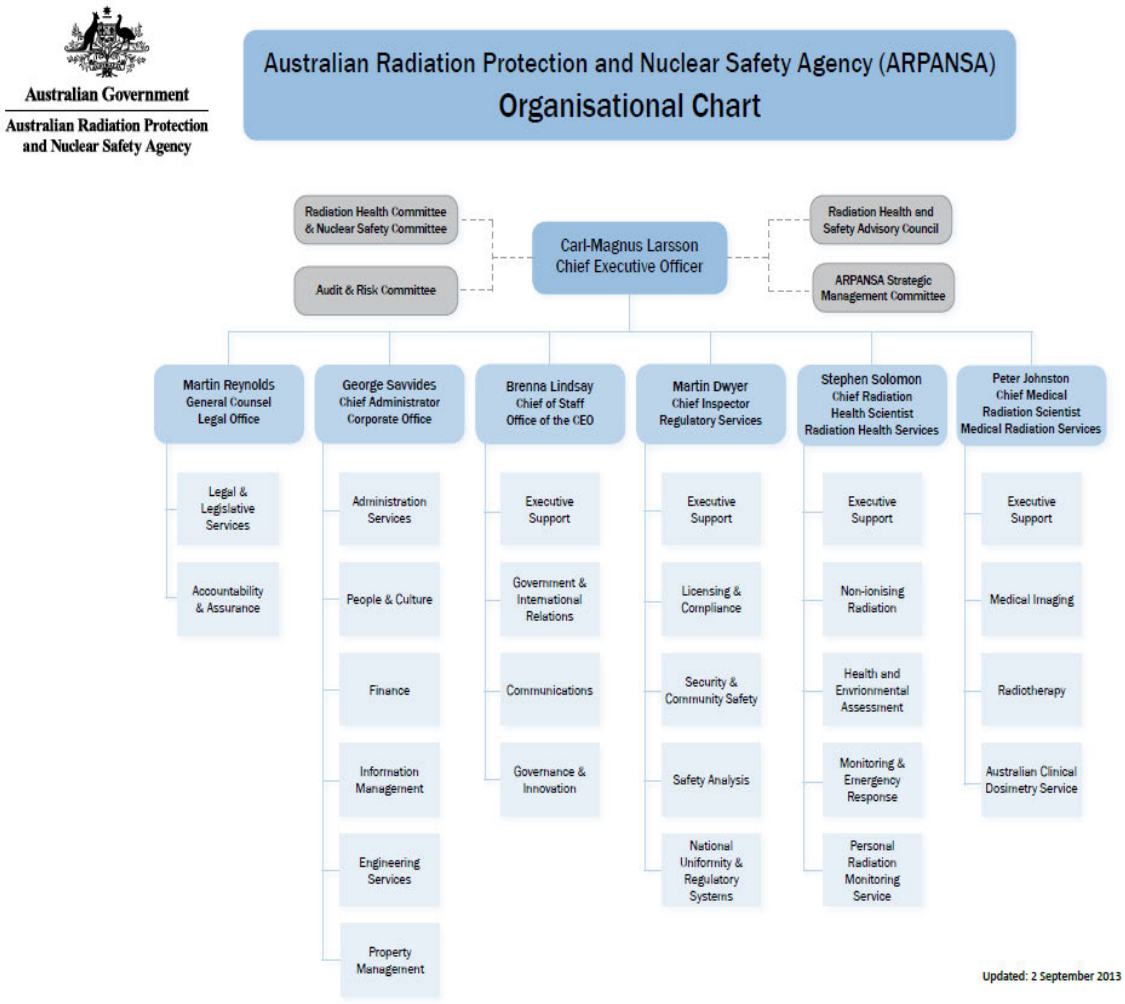
IV/B 1 Authority, Resources & Independence

The office of the Chief Executive Officer (CEO) of ARPANSA is established under section 14 of the *Australian Radiation Protection and Nuclear Safety Act 1998* (the ARPANS Act). Under the ARPANS Act, the CEO may engage staff to assist the CEO perform his statutory functions. Together, the CEO and staff constitute a statutory agency for the purposes of the *Public Service Act 1999* and a prescribed agency under the *Financial Management and Accountability Act 1997* within the Health and Ageing Portfolio.

ARPANSA is charged with responsibility for protecting the health and safety of people, and the environment, from the harmful effects of radiation (ionizing and non-ionizing). In relation to security of radioactive materials, ARPANSA:

- promotes uniformity of security policy and practices across jurisdictions of the Commonwealth, the States and the Territories and regulates the Commonwealth's use of radiation and nuclear technology;
- provides advice to license holders and jurisdiction authorities at request;
- accredits persons with technical expertise for the purposes of the ARPANS Act; and
- represents Australia in international forums that develop new principles and practices in security of radioactive materials.

Figure 1 – ARPANSA organizational chart.



IV/B 2 Regulatory Requirements and Guides

The Radiation Protection Series is published by ARPANSA to promote practices which protect human health and the environment from the possible harmful effects of radiation. ARPANSA is assisted in this task by the Radiation Health and Safety Advisory Council, which reviews the publication program for the Radiation Protection Series and endorses documents for publication, and by the Radiation Health Committee, which oversees the preparation of draft documents and recommends publication.

There are four categories of publications in the Radiation Protection Series:

- Radiation Protection Standards set fundamental requirements for safety. They are prescriptive in style and may be referenced by regulatory instruments in State, Territory or Commonwealth jurisdictions. They may contain key procedural requirements regarded as essential for best international practice in radiation protection, and fundamental quantitative requirements, such as exposure limits.

- Codes of Practice are also prescriptive in style and may be referenced by regulations or conditions of licence. They contain practice-specific requirements that must be satisfied to ensure an acceptable level of safety and security in dealings involving exposure to radiation. Requirements are expressed in 'must' statements.
- Recommendations provide guidance on fundamental principles for radiation protection. They are written in an explanatory and non-regulatory style and describe the basic concepts and objectives of best international practice. Where there are related Radiation Protection Standards and Codes of Practice, they are based on the fundamental principles in the Recommendations.
- Safety Guides provide practice-specific guidance on achieving the requirements set out in Radiation Protection Standards and Codes of Practice. They are non-prescriptive in style, but may recommend good practices. Guidance is expressed in 'should' statements, indicating that the measures recommended, or equivalent alternatives, are normally necessary in order to comply with the requirements of the Radiation Protection Standards and Codes of Practice.

In many cases, for practical convenience, prescriptive and guidance documents which are related to each other may be published together. A Code of Practice and a corresponding Safety Guide may be published within a single set of covers.

All publications in the Radiation Protection Series are available for public review and comment during drafting, and Radiation Protection Standards and Codes of Practice, which may serve a regulatory function, are subject to a process of regulatory review.

The Code of Practice on Security of Radioactive Sources (published in 2007) applies to a person dealing with a sealed radioactive source by establishing a mixture of performance based and prescriptive security requirements. In more details, this particular code can be applied to facilities, sources and any dealings, including storage, use, disposal and transportation. The Code only requires additional security measures, other than reporting of security breaches, for Category 1, 2 and 3 sources because the security measures in place for safety purposes are considered adequate to ensure the physical security of Category 4 and 5 sources. Each Category 1, 2 and 3 source will be subject to a security plan that must be endorsed by an assessor accredited by the regulatory authority. Security plans required by the Code are in accordance with IAEA requirements.

Basis:

NSS14 paragraph 1.13 - The publication applies to the security of radioactive material…Such radioactive material includes … unsealed radioactive material and radioactive waste.

Recommendation 6:

The Australian Government should develop security requirements for unsealed sources and wastes in harmony with the requirements established in IAEA NSS No.14.

Due to the division of security related regulatory tasks between ASNO (nuclear materials and associated facilities) and ARPANSA (radioactive materials and associated facilities) the regulator responsible for the supervision of radioactive materials, which are nuclear material at the same time (e.g. Pu-Be sources, irradiated U samples) is unclear currently; nevertheless the amount of such materials is minor.

Suggestion 5:

The Australian Government should consider developing clear requirements for material that is both radioactive and nuclear at the same time.

The Code of Practice on Security of Radioactive Sources prescribes, in several places, that "at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of the intrusion, and for a guard or police service to interrupt unauthorised removal of the source."

Suggestion 6:

ARPANSA should consider reformulating the general requirement for security of radioactive sources in the Code of Practice to reflect requirements for sufficient delay after detection to allow effective response.

IV/B 3 Licensing/authorization process

The CEO of ARPANSA issues licences to controlled persons to undertake certain activities in relation to controlled facilities (such as research reactors) or to deal with controlled apparatus (such as X-ray machines) and controlled material (such as radioactive sources).

In reviewing an application for a particular licence, the CEO will take into account the advice provided by his regulatory officers contained in a Regulatory Assessment Report (RAR) and other information, such as public submissions. The RAR considers the applicability of ARPANSA Codes and Standards and of particular relevance is ARPANSA Radiation Protection Series No. 11 (RPS-11), Code of Practice for the Security of Radioactive Sources. Licence applicants are required to demonstrate compliance with RPS-11 in order to gain and maintain a licence.

There are numerous Radiation Protection Series (RPS) documents and many contain security requirements specific to the particular dealing, facility or apparatus. However, RPS-11 provides the fundamental requirements for the security of radioactive sources. All RPS documents are incorporated by reference in the National Directory of Radiation Protection in cooperation with all States and Territories. Once a RPS document is incorporated by reference into the National Directory, every Australian jurisdiction must adopt it as law in its jurisdiction. This mechanism is how ARPANSA promotes national uniformity in radiation protection and nuclear safety.

Upon considering a number of matters relating to the licence application, the CEO of ARPANSA then writes a Statement of Reasons for his decision to either grant a licence or refuse to grant a licence. The CEO usually writes a Statement of Reasons only for facility licence decisions involving large facilities with significant radiological holdings. It is not normally written for the issue of source licences. Section 35 of the ARPANS Act states that the CEO may impose conditions on licences either at the time of issuing the licence or at any time after a licence is issued. This can include security requirements or emergency, preparedness and response requirements and is a powerful tool for ensuring that ARPANSA's requirements are met. In the case of Category 1-3 radioactive sources the user, based on the threat provided by the police or the regulatory body, should prepare a source security plan that is endorsed by an assessor accredited by ARPANSA. So far, ARPANSA is the only accredited assessor, thus all security plans are seen and endorsed by the regulator, but from December 2013, accredited private entities can assess and endorse security plans on behalf of the state or territory regulator.

Suggestion 7:

ARPANSA should consider taking appropriate steps to retain the regulatory role delegated to it by the ARPANS Act.

The IPPAS team noted that the Source Security Plan of ANSTO (prepared on 16 October 2013) is not in conformity with the Code of Practice.

The license for an activity covers the maximum activity allowed by the source user and the safety requirements are in relation to this licensed maximum activity. At the same time, the security requirements relate to the actual activity of the radioactive source used, stored or transported.

Suggestion 8:

The maximum licensed activity should provide basis for both safety and security arrangements.

IV/B 4 Register of Sources

The National Sealed Source Register (NSSR) is a database of ARPANSA and eight State and Territory radiation regulators. The NSSR provides a secure, centralised repository for details of all Category 1, Category 2 and, in the future, Category 3 radioactive sealed sources in Australia. A national register does not exist for the users of unsealed sources and radioactive wastes.

The NSSR uses an automated process to regularly upload data from selected Radiation Regulators with an ability to run uploads on an on-request basis. Other Radiation Regulators will update their information directly on the NSSR through a secure Web interface.

All Radiation Regulators have access to their own data through the NSSR, allowing them to review the information they have provided, as well as utilising features of the NSSR that may not be available on their systems. At this stage, there is no provision for Radiation Regulators to see records from other jurisdictions or to track transfers of sealed sources between jurisdictions.

Suggestion 9:

ARPANSA should consider continuing its efforts to include all radioactive sealed sources having activity above the D value into the national register, and provide ability to track the transfer of sources between jurisdictions as well as between jurisdiction and Commonwealth-source users.

IV/B 5 Inspection and reinforcement

The ARPANS Act includes provisions for compliance monitoring and enforcement by the CEO or inspectors appointed by the CEO. These include:

- Section 41: CEO may give a range of directions to controlled persons.
- Section 62: Arrangements for the appointment of inspectors.
- Section 63: Powers available to inspectors for monitoring compliance.
- Section 65: Powers available to inspectors for dealing with hazardous situations.
- Sections 66 to 81: Search, warrant and seizure provisions.

The ARPANSA staff include inspectors for safety and radiation protection as well as security advisors. Security advisors have no right to conduct individual inspections. Commonwealth source users are inspected at least once every year by ARPANSA inspectors; sometimes just checking license conditions and Code requirements. However, sometimes the inspections involve security advisors. Notwithstanding, the formal checking and taking account of performance based requirements is not a simple task.

Suggestion 10:

ARPANSA should consider providing the same authority to security advisors to conduct inspections on the compliance with security related requirements. At the same time, in order to benefit from safety-security synergy and optimize human resources, ARPANSA should consider training inspectors to have sufficient expertise on both safety and security areas.

V. INTEGRATION & PARTICIPATION OF OTHER ORGANIZATIONS

In addition to ASNO and ARPANSA a number of other (both on a federal and a state level) Government organizations are involved in nuclear security related issues.

The Australian Federal Police (AFP) is, based on a Government decision, responsible for guarding services involving critical infrastructure, such as ANSTO research reactor. The conditions of these services are detailed on a contractual basis between AFP and ANSTO. It may, as necessary, exercise powers stemming from its law enforcement authority.

Response forces include local state Police and their counter terrorism tactical capability and in the most serious cases, the Australian Defence Force.

The Australian Government Security Vetting Agency (AGSVA) within the Department of Defence is the central agency for the processing, evaluating and granting of national security clearances for the Commonwealth.

The Australian National Threat Assessment Centre (NTAC) issues threat assessments to inform the police and other agencies with a role in protecting Australians and Australian interests about threats to national security.

The Australian Security Intelligence Organisation (ASIO) is responsible for collecting, analysing and reporting intelligence on threats to security.

Good practice 2:

The Australian Government has established and maintains a security hotline where anyone can report any potential security events.

ASIO – T4 Protective Security section provides advice and training, technical surveillance counter-measures, physical security certifications, protective security risk reviews and physical security equipment testing.

The Australian Signals Directorate (ASD) is responsible for the Australian Government information, communication and technology (ICT) security policy and standards.

Computer Emergency Response Team (CERT) Australia, a part of the Federal Attorney- General's Department, provides the private sector with information and assistance to help them protect their Information and Communications Technology infrastructure from cyber threats and vulnerabilities. It plays a coordination role during a serious cyber incident.

The security classification assigned to information in the nuclear industry is in accordance with guidance found in the PSPF, designed for use by all departments across Government and based on the impact of compromise. As such, it is not of a nuclear or radiological specific nature, and it was stated by several of those interviewed that the guidance was subjective and open to wide interpretation.

Suggestion 11:

The Australian Government should consider producing a classification guide that is more specific and relevant to nuclear and radiological issues.

Outside of the scope of this document, but nevertheless of some concern for the IPPAS team, there appear to be differing standards applied to information security at Commonwealth and State level, and between Government agencies and private contractors. For example, documents such as the Source Security Plan (SSP) are deemed to be sensitive documents. The information they contain includes a

description of the security arrangements in place at a facility, building plans and details of persons from whom further information can be extracted.

Commonwealth regulated Government agencies are required to appropriately classify SSPs; however, the team was informed that the Government classification system does not apply a priori to private contractors. Nevertheless, ANSTO ensure that contractors are contractually bound to adopt exactly the same PSPF security standards that they themselves must adopt, and ANSTO security staff conduct inspections to ensure this happens. There are entities that are not regulated by ASNO or ARPANSA that may apply a different commercially sensitive marking to documents because they don't have the accredited arrangements to handle information that attracts a high Government classification.

Protection measures for the SSP reflect whatever system is in place in the individual State. In cases where the system does not support the National Security Classification of CONFIDENTIAL, the SSP is usually classified as COMMERCIALLY SENSITIVE and marked FOR OFFICIAL USE ONLY at the top and bottom of every page. All SSPs must also display a security caveat on the front cover.

Thus, licensees are able to adopt different standards of information security, dependant on whether they are Commonwealth or State regulated, a Government agency or private contractor. It is the infrastructure available to them that dictates the standard of security, not the sensitivity of the information itself. The Government agency regulated by Commonwealth is subject to the full force of the PSPF and all the various associated tiers of regulation; they are required to produce, handle and store their SSP in accordance with the Australian Government standards for CONFIDENTIAL information. All those who require access to the information require a mandated level of national security vetting. However, most contractors, especially those regulated at State level, are not required to adopt these standards. If the SSPs from two different licensees but containing similar information were compromised, the scale of the security breach and the damage caused would be equal. However, the security requirements and punitive measures in place for the Commonwealth regulated agency would be far more stringent than the measures in place for a State regulated contractor.

Basis:

NSS13 FUNDAMENTAL PRINCIPLE L: Confidentiality: — The State should establish requirements for protecting the confidentiality of information, the unauthorised disclosure of which could compromise the physical protection of nuclear material and nuclear facilities.

Recommendation 7:

The Australian Government should ensure a uniform approach to information security for all regulated licensees/permit holders.

VI. THREAT ASSESSMENT & DESIGN BASIS THREAT

Australia's first Design Basis Threat (DBT) from 1990 concentrated on a hostage scenario and theft of HEU from the HIFAR facility. The terrorist attacks of September 2001 and other terrorist attacks like the "Bali-bombings" which featured a Vehicle Borne Improvised Explosive Devices were the reason to review the DBT. The other factor in 2002 was that the OPAL reactor was under construction and required long term guidance to make best use of security-by-design.

The DBT was recently revised. The DBT covers the ANSTO Lucas Height site, in the design and implementation of the facility's physical protection system. Consideration was given to the various types of adversaries (i.e. outsiders, insiders and outsiders in collusion with insiders) their tactics, actions, motivation, adversary capabilities and threat information, including a set of scenarios an adversary might use to conduct radiological sabotage.

Since the decommissioning of the HIFAR research reactor no category I nuclear material at ANSTO is used or stored. Australia's determination of high radiological consequences has not yet been determined. Australia has nevertheless decided to continue with a DBT instead of a threat assessment.

Threat information from a wide range of classified and open sources and information from the operator was compiled into a number of discrete threat profiles and compositions that need to be addressed by the operator. Using the interagency process, the threat profiles were culled by removing those bounded by stronger threats and distilled into a composite threat profile. This profile was used to develop the new DBT. The 2012 approved DBT considers the insider threat, cyber security issues and airborne threats.

It was stated by the competent authority that the IAEA methodology for the design and maintenance of a DBT was followed during the DBT review and update process.

The 2012 DBT included a cyber-security component for the first time. The cyber-attack is an important issue and was considered in the actual DBT. Given the nature of this threat vector, it is highly probable that the characteristics and attributes of this threat stream will require review and update at a frequency far higher than that of the other threat streams defined in the DBT.

Suggestion 12:

The Australian Government should consider a more regular review of the DBT to take into account the changing threat environment.

_____

_____

_____.

Suggestion 13:

The Australian Government should consider including _____ *threats as part of its DBT.*

VII. RISK-BASED PHYSICAL PROTECTION

VII.1. Risk Based Physical Protection

Based on its DBT, ANSTO has installed a robust physical protection system and is, as a governmental organisation, using a strong system to protect the confidentiality of sensitive information. The management of ANSTO understands the importance of the security culture for the improvement of the physical protection system (PPS). A main step in reducing the consequences of malicious acts was the decision to shut down the research reactor which used HEU fuel and to install a new research reactor using LEU. This was a significant step to manage the risk. Evidence of ANSTO's risk based approach is clear in their Risk Management Plan and policy from December 2012. ASNO and ARPANSA agreed to target security risk level during OPAL licensing and agreed to consequences scales.

The IPPAS team was informed that ASNO has established a review process to validate the currency of the DBT.

VII.2. Graded Approach

The physical protection requirements against unauthorized removal of nuclear material are based on the categorization table given in NSS13, chapter 4. The adequacy of measures and the effectiveness of the physical protection system at ANSTO for each category are evaluated against the DBT.

Concerning the risk of sabotage, the physical protections system has been designed in such a way that an attempt of sabotage will not lead to radiological consequences beyond the thresholds set for safety. As it has been noted earlier, a clear definition of Australia's threshold of unacceptable and high radiological consequences is missing.

VII.3. Defence in Depth

The competent authorities require a layered approach for physical protection for ANSTO, which reflects the concept of several layers and methods of prevention and protection against malicious acts and their consequences. The requirements for the qualifications of the facility personnel, including trustworthiness checks, and sanctions for violation of the regulations, are layers to prevent malicious acts. The consideration of physical protection issues in the selection of the type of the research reactor (LEU) added an additional layer of defence in depth. The protection of the OPAL reactor against sabotage or unauthorized removal of nuclear material follows a multiple layer system for detection and delay of malicious acts.

VII.4. Balanced Protection

During the visit of the ANSTO facility, the IPPAS team observed that, for some buildings, the minimum time to penetrate through barriers and the minimum probability of detecting penetrations are inconsistent.

Suggestion 14:

ANSTO should consider applying the principle of balanced protection in the design of its physical protection system according to IAEA TECDOC-1276.

VIII. SUSTAINING PHYSICAL PROTECTION REGIME

Australia, at a Commonwealth level, takes relevant steps to participate in all security related initiatives and plays a significant role in the implementation of international obligations. The security experts are internationally acknowledged and the domestic training programmes are excellent. Nevertheless the professionals participate in international training programmes either as students or lecturers.

The unique nature of Australia, having only one nuclear facility, and the above described commitment of the Australian government and government organizations guarantee the maintenance of the necessary support to nuclear security related issues.

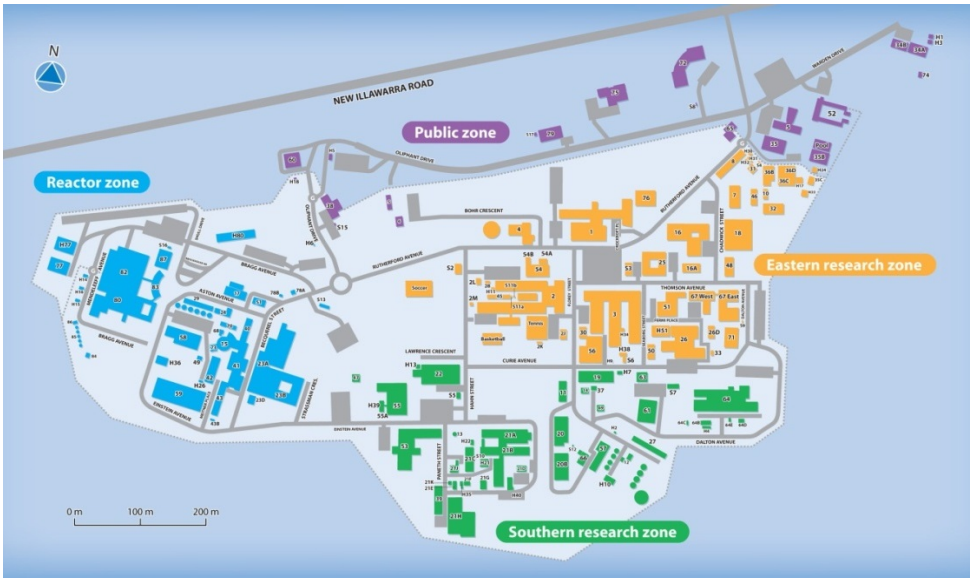
IX. FACILITY IMPLEMENTATION OF PHYSICAL PROTECTION SYSTEM AT ANSTO

IX.1. ANSTO in General

IX.1.1 About ANSTO

ANSTO is located in southern Sydney, 28 km from the Sydney central business district.

Figure 2 – ANSTO Lucas Heights facility map.



For 60 years, the Australian Nuclear Science and Technology Organisation (ANSTO) has been the home to Australia's nuclear expertise. ANSTO's recent research achievements include studies into miniature detectors to aid hadron therapy for cancer patients; research on ice and stalagmites; work that is helping understand the mechanisms behind magnets and ferro-magnetic fields; and studies into new ways to diagnose stroke and degenerative neurological diseases.

ANSTO has over 1200 researchers, engineers and support staff and more broadly accommodates on average over 1800 visiting researchers from other Australian research organisations and international research centres each year.

ANSTO operates landmark research facilities across three locations including Lucas Heights (Research Reactor), Camperdown in Sydney (Cyclotron) and Clayton in Melbourne (Synchrotron). ANSTO also operates two particle accelerators, STAR and ANTARES. There are over 120 buildings on the 70 square hectare site. At the heart of ANSTO's research capabilities is the OPAL reactor. OPAL is used for scientific research, the production of medical radioisotopes, and the irradiation of silicon used in microelectronics, in superfast trains and hybrid cars. OPAL facilitates specialised research using a growing suite of neutron beam instruments at ANSTO's Bragg Institute where scientists apply neutron scattering and X-ray techniques to solve complex research and industrial problems such as developing renewable, clean energy technologies. The Australian Synchrotron is a research facility that uses accelerator technology to produce a powerful source of light – X-rays and

infrared radiation. ANSTO is central to Australia's nuclear medicine manufacturing capabilities. ANSTO delivers doses of nuclear medicines to hospitals and medical practices across Australia.

The minerals industry relies on ANSTO to provide advice and technology to handle naturally occurring radioactive materials in mineral processing. ANSTO also provides expert advice on the safe treatment and disposition of nuclear waste and specialised irradiation services.

ANSTO is highly regarded in a highly complex area of expertise and it provides quality advice to the Federal Government on all matters relating to nuclear science, technology and engineering.

ANSTO supports Australia's international roles and obligations, contributing to nuclear non-proliferation and making sure Australia contributes to international decision making about nuclear science and technology and related applications.

ANSTO is also acting in nuclear security in the areas of nuclear forensics, detector technology for border protection and nuclear non-proliferation to promote the peaceful uses of nuclear energy.

IX.1.2 ANSTO Act

ANSTO is subject to the provisions of various commonwealth acts and regulations. The principal Act for ANSTO is the Australian Nuclear Science and Technology Organisation Act 1987 (ANSTO Act) which details the organisation's functions, powers, Board, Chief Executive Officer's duties, staffing, finance and other roles and responsibilities.

IX.1.3. OPAL Reactor

Australia's Open Pool Australian Light-water (OPAL) reactor is a state-of-the-art 20 MW reactor that uses low enriched uranium (LEU) fuel to achieve a range of nuclear medicine, research, scientific, industrial and production goals.

Opened by the Prime Minister in 2007, OPAL is a reactor with the capacity to produce commercial quantities of radioisotopes. While OPAL is the centrepiece of ANSTO's research facilities, the suite of neutron beam instruments housed next to the reactor building represent a significant research capability.

Figure 3 - OPAL reactor

IX.2. Threat and Target Identification

The operator has been provided with a nuclear material categorization table for protection against theft and the DBT by the regulatory body according to NSS 13.

The physical protection system for the research reactor is designed to protect nuclear material against theft and sabotage in accordance with permit requirements. ANSTO has identified all theft targets, including Category II and III nuclear materials and radioactive sources, their quantity, size, form, and their location within the ANSTO site. ANSTO has also identified equipment, system or devices, or nuclear material, the sabotage of which could directly or indirectly lead to potential radiological consequences that require vital protection taking into account safety studies. According to the national protection policy, ANSTO considered various types of adversaries and developed a set of scenarios which an adversary might use to conduct radiological sabotage. Nevertheless, the IPPAS team observed that, in some buildings, officers were not aware of the relevant security targets that were stored or used in the building.

In regard to the use and storage of radioactive sources the Code of Practice for the Security of Radioactive Sources requires the user to develop a risk-based process that identifies the credible threats to the source in relation to the "dealing" (as defined by the ARPANS Act and Regulations) and the likelihood and consequence of the threats occurring.

IX.3. Physical Protection Organization

A physical protection organization is established in ANSTO and it is under the responsibility of General Manager Security and Safeguards. The physical protection organization comprises several sub divisions that can support the operation of all systems within the ANSTO site. The ANSTO Security and Safeguards Policy sets out the framework for the arrangements by which ANSTO manages security and safeguards of its nuclear material. This policy provides the authority to these procedures and requirements. These procedures and requirements are authorised by the General Manager Security and Safeguards.

Responsibilities:

- Chief Executive Officer (CEO) is responsible for all security measures in place at ANSTO.
- General Manager Security and Safeguards is responsible to the CEO for the development and implementation of all protective security arrangements for ANSTO.
- Manager Security Operations undertakes the role of Agency Security Adviser (ASA). This person is appointed by the General Manager Security and Safeguards to provide advice on Security issues and performs the general day to day protective security and physical protection functions within ANSTO.
- Information Technology Security Adviser (ITSA) is responsible to, and reports to, the Chief Information Officer, but also provides 'dotted line' support to the General Manager Security and Safeguards. The ITSA is responsible for providing technical advice on the information technology aspects of information security, including technologies that can be used to protect electronic systems and networks.
- ANSTO General Managers, Heads of Institutes and Executive Managers are responsible for the implementation and enforcement of Security and Safeguards procedures and requirements within their divisions and institutes.

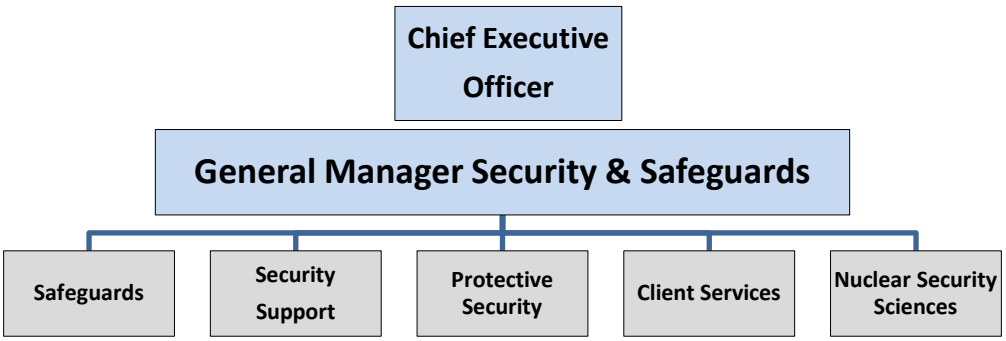
- Frontline Managers and Supervisors are responsible for leading by example, reporting security incidents, supporting Security and Safeguards procedures and requirements and ensuring their staffs are compliant with Security and Safeguards requirements.

IX.3.1. ANSTO Security and Safeguards Division

ANSTO Security and Safeguards are responsible for providing security services for all ANSTO facilities, and reception services at the Lucas Heights and Camperdown facilities. These services are provided for the protection of ANSTO and the Australian Government's staff, assets, information, facilities, materials, technology, operations and reputation. Services include (but are not limited to):

- ID pass issue and access management;
- personnel security clearance vetting;
- development and implementation of security procedures and requirements;
- provision of physical, information, and personnel security advice for all ANSTO projects, construction and operations;
- technical support to physical and electronic security systems;
- managing all contracts and tenders for security related services;
- security investigations;
- tasking of onsite Australian Federal Police (AFP);
- law enforcement, government and intelligence services liaison;
- provision of security training and awareness programs;
- security risk management;
- providing advice to Government and other national and international partners;
- regulatory compliance including Safeguards;
- facilitating project based training in radiation source security;
- security briefings for ID pass holders travelling overseas;
- threat, risk and vulnerability assessments for ANSTO operations and facilities; and,
- other security services as required.

Figure 4 - Physical Protection organizational chart



IX.3.2. Australian Federal Police / On-site Response Team

The Australian Federal Police (AFP) is contracted by ANSTO to provide a guarding force based on a government decision. AFP officers are highly trained and deployed as armed first responders to security incidents at the ANSTO site. They also conduct on-going patrols, vehicle searches on site entry and exit, monitor alarms, maintain access control and enforce Security and Safeguards procedures and requirements.

The AFP is trained to respond to security incidents, interrupt and neutralize adversaries.

The AFP also provides support to external law enforcement agencies. To allow them to carry out these duties, officers have legislated powers to stop, demand identification, search, detain and arrest.

The AFP are authorised to monitor compliance to the Security Manual by all persons upon ANSTO land including the surrounding buffer zone. All ANSTO staff are required to comply with lawful directions given by the AFP in relation to security matters or during emergency events.

IX.4. Security Procedures

ANSTO has developed and manages a suite of documents in support of its regulatory compliance and its corporate requirements. A quality management program exists to ensure documents are reviewed and updated or amended as necessary. As provided in the ANSTO Security Organisational Excellence System, documents are managed in a hierarchical structure. Within the suite are security plans, policies, procedures, and work instructions.

As a condition of permit the operator is obliged to:

- assess the proposed resource allocation, training, responsibilities, authorities and procedures at the project level, and modify them as necessary;
- delegate all authorities required;
- issue the necessary procedures; and
- determine that necessary training has been undertaken.

The security arrangements are based on the principle of defence in depth and include a mixture of hardware devices and equipment, physical barriers, procedures and administrative processes and facility design.

Security procedures cover organizational and individual expectations and duties, necessary security duties, shift deployment, protection measures, maintenance activities and expectations for incident response. Facility specific plans are developed and produced as required.

Security personnel instructions, such as access control procedures, are protected through restricted access on a need to know basis. All response force or threat intervention procedures, such as the tactical deployment plan, are classified. Physical protection procedures are developed, reviewed, implemented and enforced. All procedures and revisions that involve physical protection are approved by an appropriate level of management. Procedures are communicated to the appropriate staff through a training programme.

Verification of adherence to the written procedures is performed by the operator through an oversight process which includes monitoring of activities through supervisory oversight, key performance indicators, trending analysis, performance testing and evaluations.

IX.5. Training, Qualifications & Exercises

Security personnel at ANSTO must meet prerequisite standards for employment. Security personnel in ANSTO must undergo a comprehensive training programme to ensure that they have the skills and qualifications to perform assigned physical protection tasks and duties. Training of security personnel is adequate and on-going for response to security events. In-house and contract security personnel (AFP) receive training aligned to their duties.

Security Training at ANSTO is provided at the corporate level to all site personnel and is taken mandatorily. There is on-going refresher training and bulletins, security awareness training, information security and documentation control and guide which educate all ANSTO staff, contractors and visitors, while supporting a strong security culture.

The security guarding and response force functions for ANSTO is provided by the Australian Federal Police (AFP) who provide guarding services and are staffed to level commensurate at least with minimum staff levels described by the operator. The AFP officers trained following the federal regulations and training qualification standards. Any security personnel (AFP) who don't meet the qualifications/certifications of their posts are reassigned to other posts until they meet the requirements (i.e. firearm qualifications). Further, the AFP officers posted to the site are specifically trained to meet the unique requirements, equipment and security posts of the ANSTO facility. Verification of the training is assured through a robust program of validations, table-top exercises, performance testing and force on force exercises involving the on and off site response forces including other emergency services and multiagency response and coordination activities to assure interoperability.

IX.6. Security Culture

Nuclear security culture is accepted as the fundamental principle for effective nuclear security at ANSTO. ANSTO established a nuclear security culture strategy to further enhance the effectiveness of its nuclear security. In the promotion of nuclear security culture, ANSTO's Security Culture Strategy referred to paragraphs 32-34 of the Australian Government Protective Security Policy Framework (PSPF) specify government agency requirements for security culture and IAEA report number 7 (NSS No. 7, Nuclear Security Culture) and WINS Guidance. ANSTO employs over 1500 staff and contractors (refers to ANSTO Security Manual, AG-1028, Revision 10, Oct 2013) . In 2011 and 2012, ANSTO conducted a survey of security culture. About 500 staff participated in the survey. Nuclear security culture plays an important role in ensuring that individuals, organisations and institutions remain vigilant and that sustained measures are taken to prevent and combat the potential threat of the misuse of radioactive material to cause harm to individuals or the environment. ANSTO recognized that strong security culture is an essential human factor required to maintain protective security within a nuclear organisation. In addition to that strong security culture assists in minimising the risk of trusted insider threats and supports physical security, information security, cyber security and personnel security.

Initiatives that contribute to the security culture development programme include:

- Mandatory security reporting;
- Revised security policies and procedures;
- An enforcement regime with executive support;
- Training and awareness strategy;
- Trusted insider threat mitigation strategy;

- Organisational Excellence program;
- Recognition and reward system;
- Embedding security key performance indicators in annual performance appraisals;
- Conformance to need to know and need to share principles;
- Security requirements explicit in tenders and contracts;
- Security audits and reviews;
- Construction project consultation;
- Security and Safeguards DVD shown to all staff during mandatory security training; and,
- Raising awareness of threats to the organisation.

Good practice 3:

ANSTO conducted an on-line nuclear security culture survey to assess the level of the security culture within the organization in 2011. Based on outcomes of the survey ANSTO identified the areas needing further development to reach a more effective nuclear security. As a result of the measures introduced (i.e. security culture change programme) and the continuous endeavour of the security staff for higher effectiveness demonstrated significant improvement in security culture areas during the repeated survey conducted a year later.

IX.7. Security Plan

Several security related plans exist for different materials, their use/storage and transport, and security management issues, as follows:

- Security manual for ANSTO organizational security arrangements
- Information security manual
- Heightened security measures plan
- General plan for radioactive materials (Source Security Plan rev 0. Issued in October 2013 under the license of ARPANSA - S0045),
- General plan for transport of low category radiopharmaceutical products,
- Specific plan for transport of high category radiopharmaceutical products,
- General plan for transport of fresh nuclear fuel and uranium targets
- Investigations manual
- ANSTO enterprise risk management plan
- Crisis management plan

The different documents have different approvers and different validity. Additional procedural level documents are subordinated to the above listed plans.

Suggestion 15:

ANSTO should consider integrating the different security related plans into one security plan that will include sections dealing with the design, evaluation, implementation and maintenance of the physical protection system, and contingency plans.

IX.8. Confidentiality and Information Protection

ANSTO maintains an Information Security Management Framework (ISMF) which establishes:

- The information assets to be protected
- The technology, process and other resources which support the information assets
- The threats to those assets
- The overall risk to the assets; the risk assessment matrix in use at ANSTO was felt to be of a high standard due to its granularity and ability to achieve results that are repeatable
- The risk treatment strategies to mitigate the identified risks
- The controls selected to support the mitigation strategy
- A description of the requirements of the standard and their applicability to the service being protected
- The associated policy and procedure documents that ensure that the controls are implemented and maintained in support of the risk treatment strategies.

Overall, a good standard of information security was noted, and evidence was presented to the IPPAS team covering the following topics:

- External regulation
- Operating procedures
- A graded approach to risk management based on the confidentiality of information
- Training programmes
- ——————————————————————————————.
- The extension of company security standards to external contractors.

In accordance with the Australian Government Protective Security Policy Framework (PSPF), which is a licencing and permit stipulation from both ASNO and ARPANSA, all information that has been assessed as sensitive is segregated and controlled under strict need to know arrangements. Such information would include; the Site Security Plan (which contains a section on specific security concerns and possible weaknesses), various safety related documents and other documents of a sensitive nature, including certain engineering drawings.

ANSTO operate a number of standalone laptops specifically to process sensitive information with a higher confidentiality requirement. The laptops are strictly controlled, available for use only by suitably cleared (in accordance with the PSPF) individuals, fitted with Australian Signals Directorate (ASD) approved hard disk encryption and secured in Australian Government Security Construction Equipment Committee (SCEC) approved containers when not in use. Physical security inspections are carried out by T4 Section of the Australian Security Intelligence Organisation (ASIO), who are responsible for certification of some physical security infrastructure. Dissemination of more sensitive information is in hard copy, and only to those with a genuine need to know and with suitable security containers to secure it.

Almost all contractors who carry out work for ANSTO do so at the licenced site. They are obliged to adopt ANSTO security regulations, and this is made explicit to them at the tender stage of a contract. A small number of contractors are allowed to work on ANSTO information at their own locations. In order to be able to do this, security arrangements at their business premises are first inspected by a member of the ANSTO security team, to ensure that adequate security standards are in place.

IX.9. Cyber Security

Overall, a good standard of cyber security was noted, and evidence was presented to the IPPAS team covering the following topics:

- external regulation
- operating procedures
- a graded approach to risk management based on threat and the confidentiality, integrity and availability of systems and data
- training programmes
- network segregation and configuration management.

The information security standards that ANSTO apply are in accordance with the Australian Government's Information Security Manual (ISM), which forms part of the Protective Security Policy Framework (PSPF). It is a stipulation of both ARPANSA licencing and ASNO permit conditions that the PSPF must be adhered to. In addition to the seven mandatory controls related to information security within the PSPF top level document, over 700 possible controls in the ISM may be used within a risk-based framework to secure computer assets.

ANSTO has not implemented every single control in the ISM; nor are they required to within a risk-based approach. In each case where a particular control has not been applied, the risk has been assessed, mitigating factors have been taken into account and the residual risk accepted in the form of a non-compliance grant by the CEO.

External regulation of cyber and information related security measures is carried out by several competent agencies, most notably ARPANSA; ASNO; the Australian Security Intelligence Organisation (ASIO); the Attorney-General's office; and Australian Signals Directorate (ASD).

ANSTO operates [redacted] networks for security and instrumentation and control (I&C) systems. [redacted]. In addition to this, nuclear material accountancy and control is carried out on standalone equipment with no external connections, which can be suitably secured when not in use.

Figure 5 - ANSTO Information Technology Network Environment Overview

Separation between the various different networks appeared to be of a generally good standard, [redacted]. It is assessed that there are adequate physical, technical, personnel and procedural measures in place to provide defence in depth, prevent data migration and malicious infection.

The primary ANSTO network used to process information of a commercially sensitive nature (known as IN-CONFIDENCE) is ANSTONET, located primarily within ANSTO's Lucas Heights site, [redacted]. The network provides a number of services such as email, internet access, file storage and remote user access. ANSTONET is self-accredited by the CEO of ANSTO, but only after ANSTO's Information Technology Security Advisor (ITSA) has audited and certified the network as suitable for accreditation. (It is understood, but not confirmed, that every Federal Government Agency also has an ITSA.)

Remote user access to ANSTONET is permitted from both company-owned laptops and privately-owned PCs (limited access only) belonging to company employees. This is inconsistent with what is described in the ANSTO Information Security Manual. Dual authentication is required for remote access in the form of a remote access token, combined with user name and password. The company is also trialling a Juniper based solution that will provide read-only access. Privately owned USB sticks are not allowed to be used on ANSTONET;[redacted].

[redacted].

[redacted]. [redacted] has been accredited by ASD, the Australian Government competent computer security authority. A stipulation of continued ASD accreditation is that the network must be subject to external auditing by ASD endorsed consultants registered under the Information Security Registered Assessors Program (IRAP) every two years. In the interim years, the network is subject to internal audit by the ANSTO ITSA. There is no ASD or regulatory requirement to conduct a penetration test (Pentest) of the network; however, ASD are available to carry out such a test at no cost if this is deemed necessary.

[redacted], but this is through an ASD accredited one-way data diode, and no data can enter [redacted] by this means. The connection is strictly limited to a small number of user terminals that are locked down [redacted]. Strict Change Control procedures have been adopted for [redacted], and the network has its own dedicated IT team with in-depth I&C knowledge. No remote access of any kind is allowed on the [redacted] network, and only dedicated equipment may be connected. This includes laptops maintained by OPAL IT staff for contractors to use.

[redacted]. Thus the analogue back-up would be unaffected, even if there was complete compromise of the RCMS and main RPS. This may have positive implications for the Impact Level of the FRPS.

Physical access to the I&C and security networks is tightly controlled, and mainly limited to protected areas.[redacted].

Suggestion 16:

ANSTO should consider requesting that ASD conduct a vulnerability assessment (penetration test) to ensure that unauthorised access between [redacted] and the [redacted] network cannot be achieved. The subsequent report should then form part of the security documentation and inform future network alterations.

Suggestion 17:

ANSTO should consider formally re-evaluating the classification of [redacted] in accordance with NSS 13, NSS 17, and PSPF Mandatory requirements INFOSEC 3 and PHYSEC 6, to ensure that they have been correctly classified commensurate with the confidentiality, integrity and availability of the data processed, and the Impact Level for each system on the networks. If this results in an increase to the existing residual risk, the network architecture and current security measures (physical, technical, personnel and procedural) should be reviewed to ensure they remain adequate.

Suggestion 18:

ANSTO should consider improving control of access to [redacted] employ two-factor authentication (i.e. proximity and PIN) at all times.

ANSTO allows company employees to use privately owned electronic devices (collectively known as "Bring Your Own Device or BYOD") on company premises (for non-work purposes). Separate wi-fi access is provided for their use, and such devices have no access to company networks.

Good practice 4:

Good practices were noted for the removal of computer equipment offsite, including the use of gate passes and hard drive encryption. All staff, contractors and visitors are required, on entry, to register and seek approval to remove any assets from the facility.

Disposal procedures for computer equipment were also deemed to be effective. It is a stipulation of the ISM that separate Security Operating Procedures (SyOPS) are provided for different types of system users, for example system administrator SyOPs are far more rigorous than the SyOPs required by a normal user, as the administrator will have more control over a system, and thus more scope to breach security regulations.

A documentation framework is required under the Australian Government ISM, including a Security Risk Management Plan, individual System Security Plans, the above mentioned SyOPs, an Incident Response Plan and a number of other documents. Many of these are still under development; however, they are broadly in line with the Computer Security Plan required in accordance with NSS 17. A number of other measures from NSS 17 were also noted, such as:

- Remote maintenance access is specifically disallowed on all networks.
- The number of staff given access to each network has been kept to an absolute minimum, and is reviewed on a regular basis. There is precise distinction between normal users and those with administrator rights.
- All connections to the I&C and security networks appear to be tightly controlled, with USB access prevented for normal users. This is enforced using technical controls, and the software used to enforce the policy has a monitoring capability. ——————————————————.
- Strict change control procedures are in place on the I&C network.
- Internet access is only possible from ——————————————.

Whilst many computers within ANSTO were running on a Windows 7 operating system, a number of ——————————————————————————; this operating system will shortly no longer be supported by Microsoft, meaning that the company will be unable to apply patches, etc. This situation was discussed with computer security staff, and it was confirmed that an upgrade —— is underway.

IX.10. Sustainability Programme

The security & safeguards division of ANSTO provided the IPPAS team with a number of documents covering:

- Operating procedures
- Human resource management
- Training and exercises programmes
- Equipment maintenance, updating and configuration management.

ANSTO has implemented a strategy for maintaining the technical parts of the physical protection system, including means for detection, assessment and access delay, access control, systems to detect introduction of prohibited items, and networks and low voltage electrical equipment required for those items above. This extensive programme includes functional tests, calibration measurements by maintenance personnel, preventive & predictive measures, analysis of system effectiveness, trending and corrective actions when necessary.

Preventive maintenance is carried out periodically, the frequency being based on manufacturers' recommendations, contractors' expertise and operational experience.

Predictive maintenance aims to minimize equipment failure and prevent corrective maintenance. The security team conducts trending of equipment events to look for generic failures and identify obsolete equipment. Predictive and preventive measures are carried out according to an annual plan. Maintenance activities comply with and are integrated in the security work management system. They are documented in security & safeguards division.

Corrective maintenance occurs in a timely manner when equipment appears to be out of order. If the defect cannot be fixed immediately, compensatory measures are implemented until completion of the repair.

Security Construction Equipment Catalogue (SCEC) endorsed products are used as a measure of quality control for the implementation of protective security.

The IPPAS team considered that:

- adequate resources are in place, including appropriately trained personnel, to enable full implementation of the conditions of the above mentioned requirements, and
- adequate levels of appropriately qualified staff maintained to ensure the system of nuclear security is fully implemented and operational at all times.

IX.11. Quality Assurance

The quality assurance policy and programmes for physical protection established and implemented at ANSTO ensure that the physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the DBT. The General Manager of the Security & Safeguards Division is responsible for the quality of the physical protection system. He reports to the Chief Executive Officer.

IX.12. Evaluation

The evaluation process aims to verify that the physical protection system is able to achieve its objectives against the DBT. The evaluation of the physical protection system is part of the security plan submitted and then approved by the competent authorities in the framework of the licensing procedure. A vulnerability assessment and target identification are included in the evaluation process.

The evaluation of the physical protection system is based on adversary pathway analysis, which has been conducted and submitted as part of the security plan to ASNO and ARPANSA for approval as part of their permit and licence condition. These approvals should precede any modifications of the physical protection system. The operator validates and demonstrates the effectiveness through exercises.

The competent authority (ASNO) carries out a significant number of visits to ANSTO each year. Normally, one visit (one or two days) is conducted every second month at ANSTO for different facilities. Of these visits, one to two inspections are carried out per year. While the timing of inspections is normally announced, the details of inspection activities are notified in advance only if necessary (for instance, to check equipment or documents); otherwise, they are not revealed until the inspection itself.

IX.13. Interface Physical Protection/Material Control & Accountancy

ASNO is authorized by the Safeguards Act to:

- initiate, activities for cooperation with IAEA and with other international organizations specialized in the nuclear field;
- control and implement the provisions of international treaties and agreements in force, with regard to safeguards, physical protection, illicit trafficking, transport of nuclear and radioactive material, radiation protection, quality assurance in nuclear field, nuclear safety, safe management of spent nuclear fuel and radioactive waste, and intervention of nuclear accident;
- establish and coordinate the national system for evidence and control of nuclear material;
- represent the national contact point of contact for nuclear safeguards, for the physical protection of nuclear material and installations.

Through permit conditions ASNO requires that ANSTO:

- Demonstrate that, for every project involving nuclear material including actions and materials associated with it, a formal documented process of identifying potential diversion scenarios for that material, including methods that could be employed and taking into account the sensitivity of the material, has taken place. The plan shall include the results of the identification process and the measures proposed by the permit holder to prevent or detect such diversion. The process and results shall be documented and reviewed both every five years and as required to respond to changes in circumstances;
- Demonstrate, via documentary evidence, that procedures are in place and are being effectively implemented to detect any loss of control of nuclear material listed on the inventory;

- Demonstrate, via documentary evidence, that the satisfactory performance of the individual segments of the MC&A system, and the system as a whole, is routinely inspected, tested and evaluated against their design specifications and corrective measures applied if necessary; and
- Demonstrate, via documentary evidence, that the performance of the MC&A system is continually monitored and assessed against these criteria, and any other MC&A related permit or licence requirements.

At ANSTO both safeguards and security report to the same General Manager and through observation it was evident that there are established processes and procedures demonstrating interface between the security and safeguards sections. These indicators include such measures as needing either security presence or notification (as required dependant on facility) for access to storage areas and requirement for both Security and Safeguards personnel to be in attendance in order to access nuclear fuel (two person rule).

Further the AFP protective force was required to be present and facility operation staff requires pre-notification of such activities ——————.

Safeguards staff conduct material accounting through various methods and is required to report to the regulator and its own security organization, any discrepancies in balances or loss of material.

Further, by condition of permit, ANSTO is required to:

- Notify the Director General of any incident involving either an actual or a suspected compromise of accountancy and control within two hours of its discovery.
- Conduct investigations into any incidents notified and provide a report to the Director General, within 10 working days of the notification of the incident, detailing the actions undertaken in the investigation, findings of investigation, actions to correct any compromise and actions taken to prevent recurrence of such incidents.

IX.14. Trustworthiness Checks

The PSPF (PERSEC 1) requires Australian Government agencies to ensure that Government employees, contractors and temporary staff who require ongoing access to Australian Government information and resources are eligible and suitable to have access, have had their identity established and are willing to comply with the policies, standards, protocols and guidelines that safeguard that agency's resources (such as people, information and assets) from harm. Access to national security classified information is dependent upon the granting of the requisite security clearance by the Australian Government Security Vetting Agency (AGSVA).

AGSVA is located within the Department of Defence and is the central agency for the processing, evaluating and granting of security clearances for the Commonwealth. It conducts clearances for the majority of Government under a fee-for-service model.

National security access controls include a system of identifying sensitive material and premises with classifications such as PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET. Only people with appropriate security clearances and an appropriate "need-to-go" are allowed access to such premises or material. The general policy and requirements for Australian government security classifications are set out in the Australian Government Protective Security Policy Framework (PSPF).

All relevant Government agencies must follow the Australian Government Personnel Security Protocol for personnel security as contained in supplementary material within the PSPF. Only AGSVA (and exempt agencies) can grant, continue, deny, revoke or vary a national security clearance.

Agencies must have in place personnel security aftercare arrangements, including the requirement for individuals holding security clearances to advise the AGSVA of any significant change in personal circumstances that may impact on their continuing suitability to access security classified resources. At ANSTO, all of these requirements are communicated to staff at annual security training and awareness sessions. PSPF personnel security requirements are documented in the ANSTO Security Manual and various other ANSTO policies and procedures.

A security clearance process is conducted to ensure that an individual is both eligible and suitable to be granted, as well as maintain, a security clearance. AGSVA will make the decision about granting a security clearance in accordance with the six mandatory requirements included in the PSPF.

All clearances granted by AGSVA are portable across all agencies (excluding exempt agencies). This single, consistent approval has improved the clearance process by:

- providing one clearance that is effective across government;
- removing inconsistencies between previous clearance processes; and
- increasing the efficiency for all parties

ANSTO employs two types of security clearances. They are:

- ANSTO (General or Protected) site access clearances (where individuals are vetted by ANSTO); and
- National Security Clearances (vetted by AGSVA).

All staff and contractors requiring unescorted access to site must undergo the ANSTO security clearance process. This requires all applicants to sign an official secrecy form, declaring an understanding of the responsibility of Commonwealth Officers to maintain official secrecy under Section 70 of the *Crimes Act 1914*. A reassessment for suitability is carried out if numerous security breaches or a security violation is conducted and at regular intervals as part of the revalidation regime. Visitors, defined as anyone who is not a staff member or contractor and will be visiting ANSTO, are issued with a visitor access pass and must be escorted by their host at all times while on site.

Good practice 5:

ANSTO has implemented an insider threat mitigation strategy. The strategy sets out a broad range of activities designed to mitigate the insider threat risk, including a comprehensive vetting process, which includes five key personnel security elements (honesty, maturity, loyalty, tolerance and trustworthiness).

IX.15. Reporting

IX.15.1 Reporting to ASNO

ASNO issues permits to operators as provided in the *Nuclear Non-Proliferation (Safeguards) Act 1987* to ensure and maintain physical protection and safeguards as licensed. The operator is required to observe the technical conditions and limits provided in the authorization and to report any violation, in accordance with the specific permit conditions. During the visit to ANSTO the IPPAS team understood that a standardized reporting procedure was established for both security and safeguard requirements.

As a condition of permit, ANSTO is required to report the following:

Security

- Report to the regulatory body any incident involving either an actual or a suspected compromise of physical security (such as breaches of security, acts of sabotage or attempted acts of sabotage) within two hours of its discovery.
- Conduct investigations into any incidents notified and provide a report to the Director General, within 10 working days of the notification of the incident, detailing the actions undertaken in the investigation, findings of the investigation, actions to correct any compromise and actions taken to prevent recurrence of such incidents.
- Report to the Director General by 31 January each year on the outcomes of the assessment of the system's performance, carried out, over the previous 12 months.
- Report to the Director General any changes to either the site assessment or the threat assessment for this facility within 72 hours of the change.

Safeguards

- Notify the Director General of any incident involving either an actual or a suspected compromise of accountancy and control within two hours of its discovery.
- Conduct investigations into any incidents notified and provide a report to the Director General, within 10 working days of the notification of the incident, detailing the actions undertaken in the investigation, findings of investigation, actions to correct any compromise and actions taken to prevent recurrence of such incidents.
- Report to the Director General by 31 January each year on the outcomes of the assessment of the system's performance, carried out over the previous 12 months.

IX.15.2 Reporting to ARPANSA

ARPANSA issues licence conditions to operators as provided in the Australian Radiation Protection and Nuclear Safety Regulations 1999, to ensure and maintain control of material and facilities as licensed. The operator is required to observe the technical conditions and limits provided in the authorization and to report any violation or breach of licence condition. Further the operator must report the following in accordance with the regulation:

- If the holder of a licence identifies a breach, the holder of a licence must rectify the breach and any consequences of the breach as soon as reasonably practicable and the holder of a licence must also tell the CEO as soon as reasonably practicable in accordance with Regulation 45.
- The holder of a licence must, at least once every 12 months, review and update any plans and arrangements for managing the controlled facility, controlled material or controlled apparatus to ensure the health and safety of people and protection of the environment. The holder of a licence must, after conducting a review, give the CEO information about the review in accordance with Regulation 50.
- The holder of a licence may make a relevant change that is unlikely to have significant implications for safety without the CEO's approval. However, the holder of a licence must, at least once every 3 months, tell the CEO about any of these changes in accordance with Regulation 52.
- The holder of a licence must only dispose of controlled apparatus or controlled materials with the approval of the CEO. If the holder of a licence transfers controlled apparatus or controlled materials to the possession of another person or body the holder of the licence must, within 7 days of the transfer, tell the CEO:

  (a) that the transfer has happened; and

  (b) the name of the other person or body; and

  (c) the number of the licence held by the other person or body; and

  (d) the location of the controlled apparatus or controlled materials after the transfer.

<u>Reporting to Police</u>

In accordance with the Code of Practice (Security of Radioactive Sources Radiation Protection Series Publication No. 11 January 2007, Section 7.1.1 (a) (v) (ii)), the responsible person dealing with a radioactive source must notify police immediately if a breach occurs involving:

- (i) detectable theft;
- (ii) unexplained loss;
- (iii) unauthorised damage;
- (iv) unauthorised access; or
- (v) unauthorised transfer,

X. ON-SITE & OFF-SITE RESPONSE

X. 1. Guards & Response Forces

ANSTO contracts the Australian Federal Police (AFP) through a Memorandum of Understanding (MOU). The AFP provides a 24 hours per day, 7 days per week (24/7) guarding service and response forces. Performance testing of the physical protection system is performed and includes appropriate exercise, for example force-on-force exercises, to determine if the guards and response forces can reach this objective at least 3 times per year in accordance with ANSTO's exercise schedule. Site Control Centre (SCC) personnel and the off-site response force communicate at scheduled intervals in accordance with the security manual. The AFP guard force conduct random patrols in the protected area; the response force provides an effective and timely response to prevent unauthorized removal of material or sabotage according to the emergency response plan. The IPPAS team were impressed with the strong relationship between the on-site and off-site response forces.

The IPPAS team recognised the challenge in maintaining the vigilance and deterring the potential complacency of the guarding force and that there was no objective quality control measures to monitor effectiveness.

Suggestion 19:

ANSTO should consider establishing a process for the independent verification of guard force performance.

Good practice 6:

The effectiveness of on-site response forces for the research reactor is regularly tested by multi-agency force-on-force exercises.

X. 2. Command, Control & Communications

The SCC initiates and receives communications using redundant, diverse means such as radio or telephone, to communicate with other members of security staff in the performance of any assigned duty. All ANSTO radio communications are encrypted. ANSTO operates - patrol/emergency response vehicles ——————————————. In addition to this, foot and bike patrols operate regularly. There is a telephone hotline to off-site AFP, State police and other emergency services operating with the SCC. ANSTO evaluates the physical protection measures and physical protection system, including performance testing and the timely response of the guard and response forces regularly to determine reliability and effectiveness against threat. ANSTO carries this out with full cooperation of the on-site response force, and if necessary, with the assistance of off-site response forces such as state police, etc.

XI. SITE CONTROL CENTRE

The Site Control Centre (SCC) is located in the limited access area. The building is based on the design specification ES 128150-A, and is hardened against the threat. Entry to the SCC is heavily restricted, and based on triple authentication, in accordance with the security manual. The IPPAS mission noted that——————————————————————————————————. The SCC is adequately equipped with alarm, surveillance, and communication capability. When an alarm is triggered in the SCC, an alarm annunciator system indicates the location of the alarm source in accordance with the design specification ES 128150-A. The CCTV system is equipped with automatic video recording and capture capability that quickly retrieves and displays footage, in accordance with the design specification ES 128150-A. A Back-up Site Control System exists. All intrusion detection alarm events including alarm assessment are automatically recorded in accordance with the design specification ES 128150-A.

Suggestion 20:

ANSTO should consider the appropriateness of current staffing levels of the SCC.

The SCC, which also acts as the transport control centre during certain transports of material, is in the process of being refurbished. It has been ergonomically designed to reduce the level of operator fatigue whilst watching screens. The SCC is the main area where alarms for the various security systems and some other control systems terminate. Full functionality of the SCC is replicated at an unmanned alternate SCC, and the local AFP station can also be used to control site emergencies at ——functionality.

AFP personnel within the SCC appeared well trained and knowledgeable of the systems they were operating. Computerised response instructions are also incorporated into the CCTV and Intruder Detection System (IDS). In the event that a certain sensor activates, the operator is alerted to the exact location on a digitised map, and response instructions specific to that location containing contact numbers and other useful information appears on screen.

Good practice 7:

Liberal use of flap sheets – laminated instructions containing the actions to be taken in the event of certain incidents. This negates the requirement for AFP personnel to trawl through larger documents when response timings may be critical to success or failure.

The SCC / CAS is equipped with a Duress or Panic Actuator Button (PAB) to request support from other AFP officers at ANSTO. In cases of emergency SCC / CAS operators can make announcements through the public address system installed in the SCC.

XI.1. Alarm Assessment

Alarms are assessed by two methods, by cameras to cover each intrusion sensor sector and by visual checks by posted guards, or patrol guards. ANSTO uses both methods. ANSTO assess the cause of an intrusion alarm by expert staff. ANSTO operate —— CCTV at the site, and this equipment is assessed as adequate and appropriate for the facility, provided that the equipment performs as designed. The alarm zone covered can be viewed effectively during daylight and night-time hours. There is no glare or blooming effects to impede assessment on the CCTV monitors, and there is no clutter, such as vegetation or construction materials, in the field-of view to impede assessment within the protected

area. The picture quality of the CCTV system is appropriate to monitor persons or activities anywhere within the field-of-view.

The outdoor CCTV cameras are appropriately protected from the environment in accordance with the PSPF Guideline (Section 5.10). CCTV lenses are maintained according to a maintenance schedule and contract. The design specifications contain minimum performance criteria.

The IPPAS team observed that the effectiveness of the facial recognition techniques could be improved as the current system is limited to a human comparison of photos with the image projected on the assessment device.

ANSTO operates a duress alarm system, ———————————— of the Automated Access Control System (AACS). When triggered, a duress call is sent to the SCC. In order to address the insider threat, ANSTO operates an awareness program, which all are briefed on regularly. Security exercises also now include the insider threat, based on the 2012 DBT.

XI. 2. Emergency Power

—— different sources provide power to the physical protection system. They switch on automatically and immediately in the event of loss of normal power. All alarm and assessment systems remain operable from uninterruptible power sources (UPS), and a UPS is also connected ———————————————. It is tamper protected, and the UPS is regularly tested and maintained. ANSTO is supplied by emergency power at each building. Emergency power supply is provided to alarm equipment, alarm communication equipment and the SCC, in order that they can remain operable during any situation. The duration of Emergency power supply is sufficient for transfer from normal to emergency power.

XII. OUT OF FENCE & FROM PERIMETER FENCE TO BUILDINGS

In all areas seen, the external perimeter to ANSTO consisted of a double fence of at least 2.4m of chainlink topped with three strands of barbed wire. The lack of rigidity of chainlink fences makes them unsuitable for use with many types of Perimeter Intrusion Detection Systems (PIDS), although it was noted that a microphonic system is mounted on some areas of the fence, with no apparent problems experienced. Lighting was considered by the team to be acceptable, but this cannot be assessed with any accuracy until a full lighting survey to measure lux levels is conducted. This is outside the scope of the IPPAS Mission.

Hostile vehicle mitigation measures at the main gate were assessed as effective. Rising bollards, approved by ASIO T4 Section and crash tested to the PAS 68 standard are installed. A reject lane diverts unauthorised vehicles away from the gate before they reach the bollards, and before they can access the site. An electronic sliding gate to the other side of the guard hut is also assessed to be constructed and installed to the PAS 68 standard.

In the area of perimeter fence next to the Discovery Centre is a pedestrian double turnstile. It appears that this area was once a vehicular access point that is no longer commissioned for that purpose, other than for emergencies. A large planter has been placed across the external area of fence to prevent hostile vehicle attack; if the planter has been anchored correctly, it should constitute an effective barrier.

In the area around building —, a full height electric fence has been fitted on the inner perimeter fence instead of the normal barbed wire fence-topping. From a distance, the electric fence appeared to be in very good condition, , especially when combined with the coiled razor wire that has been placed in the sterile zone in this area.

ANSTO is in the process of upgrading the existing Closed Circuit Television (CCTV) system around the perimeter, and the upgrade is approximately 25% complete. The newer system is far more sophisticated, and incorporates both optical and thermal fixed and PTZ cameras. The software is equipped with advanced analytics that allows all cameras to be used for motion detection eliminating the need for functionality at the edge (camera). The detection parameters for each individual camera are fully customisable. The new CCTV system has the ability to record up to 90 days' worth of footage. The most recent footage is stored at a high pixel rate at 13 frames per second (fps), but there is a graduated reduction in image quality and fps as the footage gets older.

Suggestion 21:

ANSTO should consider prioritising the programming of detection analytics for building —.

Good practice 8:

The principle of long range detection was observed through the use of technology, which far exceeded the protected area boundary.

XIII. OPAL

Australia's Open Pool Australian Light-water (OPAL) reactor is a state-of-the-art 20 MW reactor that uses low enriched uranium (LEU) fuel to achieve a range of nuclear medicine, research, scientific, industrial and production goals. While OPAL is the centrepiece of ANSTO's research facilities, the suite of neutron beam instruments housed next to the reactor building represent a significant research capability.———————————————————————————————.

Figure 6 – OPAL reactor pool

XIII.1. Detection System

The OPAL facility is equipped with a perimeter intruder detection system (PIDS). PTZ cameras provide good surveillance coverage of the OPAL site, and external lighting is installed to support camera operation. All alarm communications associated with the PIR and CCTV cameras terminate at the Site Control Centre (SCC) / Central Alarm Station (CAS).

———————————————————————————————
———————————————————————————————
———————————————————————————————
————————————————————————————.

Inside the OPAL building, good coverage was noted from the intrusion detection system (IDS) and CCTV system. In order to gain access to OPAL, staff must inform the AFP operator in the SCC/CAS.

The main entry point at OPAL is controlled by CCTV and an automated access control system (AACS).

Suggestion 22:
ANSTO should consider improving the effectiveness of access and egress control with respect to unauthorised object detection capability for protected areas.

XIII.2. Delay System

The OPAL site walls, windows and portals provide delay into the protected area. In addition, OPAL has an iron cage fitted to the roof to protect the building from hostile aircraft.

An integrated system of defence in depth is in place at OPAL. A guard post is located in the protected area boundary; the building is also equipped with AACS, and to enter the OPAL protected area it is necessary to gain access through the SCC, which operates 24 hours per day/ 7 days per week (24/7). Staff who are authorized can use their AACS pass to gain access.

XIV. BUILDING —

Building ——— is a facility where —— waste ——————————————————— is stored. It has a largely corrugated iron/breezeblock construction. Entry to building — is via a compartmentalised Automated Access Control System using both proximity pass and PIN. Personnel requiring access must also telephone the SCC to be verified with the AFP. AFP operators at SCC/CAS monitor this area 24/ 7. The team were informed that the building has been fitted with an Australian Government SCEC (Security Construction Equipment Committee) Type 1 Intruder detection System (IDS), ——.

***Figure 7* – Building —**

——.

Perimeter patrols of all buildings are conducted, including the outer perimeter of this facility; ——. External lighting consisted mainly of bulkhead lights, but these were assessed as adequate, given the role of the building.

External lighting and exterior CCTV were both assessed as adequate.

The fence around building — consisted of 2.4m chain-link topped with three strands of barbed wire. In addition to this, a coil of razor wire had been placed on the ground inside the fence line in all areas except the palisade gate, which was of a good security standard. ——.

XV. BUILDING —

Building — is a storage building for nuclear material less than Category III. It is a limited access area with a largely corrugated iron/breezeblock construction.[redacted].

Figure 8 – Building —

There was no fence around building —. Entry to the building is via a compartmentalised Automated Access Control System using both proximity pass and PIN. Personnel requiring access must also telephone the Site Control Centre (SCC) to be verified with the AFP using a CCTV system at the entrance.

External lighting was assessed as adequate, and there are two dedicated CCTV cameras covering opposite sides of the building including the fire exit. A number of long range PTZ cameras are also capable of providing coverage to this area if required, although they don't appear to cover it in their normal at-rest position.

Internally, the building has an Australian Government SCEC (Security Construction Equipment Committee) Intruder detection System (IDS),[redacted]. Internal CCTV cameras share the same [redacted].

XVI. BUILDING —

Building — is a facility that produces Mo-99 by dissolving irradiated uranium plates; it is a Category III facility which is permanently staffed, 24/7. ————————————————————.

Suggestion 23:

Building — would benefit from external CCTV in order to verify any alarms triggered by unauthorized access.

Entry to building — is via a compartmentalised Automated Access Control System (AACS) with proximity pass, and this is extended to the operational area inside the building. The AACS terminates at the SCC operated by AFP. The AACS covered all external entry and exit doors to the building, including fire exits, which were signed to indicate they were alarmed. Once inside the operational area, there is no further control of access between the ground floor hot cells area and the upstairs control room. Nor is this considered necessary, as all staff within the hot cells area have a potential requirement to access the control room.

There is no fence around building —. External lighting consisted mainly of bulkhead lights, but these were assessed as adequate, given the role of the building.

XVII. BUILDING ——

Building —— is a dry storage facility containing material categorized as below Category III nuclear material and therefore, in accordance with NSS 13, the material should be protected at least in accordance with prudent management practice.

Door passages (pedestrian and vehicular) are equipped with magnetic reed contact switches which provide audible and signal alarm to the SCC. Pedestrian doors are equipped with — locks. The pedestrian doors are designed to fail safe and egress may be achieved through breakage of a glass covered control allowing emergency exit. Breakage of this equipment results in an alarm to the SCC.

The building is equipped internally with an Intrusion Detection System (IDS), ————————————————————.

Entry to the building is gained by use of a proximity card and PIN. Personnel requiring access must also telephone the SCC to be verified with the AFP.

The facility is constructed of metal clad on slab building with a comparable roof material mounted on steel girders. Pedestrian access doors are metal clad and the facility is equipped with a metal roll up vehicular access doorway. The facility contains no material handling equipment therefore greatly extending the adversarial task time or equipment needs in accessing material in this facility.

XVIII. BUILDING [redacted]

The building is located in a limited access area and hosts the radio-pharmacy production activities of ANSTO. The major products of the facility are molybdenum/technetium generators and I131 however other isotopes are also produced in smaller scale. [redacted].

The building also accommodates an interim storage pond for spent [redacted] sources.

[redacted]. The entrance doors are security doors, equipped with security locks. Windows are equipped with security grills.

Basis:

NSS14 paragraph 4.11 - Detection measures should be implemented for the discovery and assessment of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of radioactive material.

Recommendation 8:

ANSTO should apply detection measures on potential adversary routes into the radiopharmaceutical production facility by-passing the routes currently covered by detection measures.

XIX. BUILDING [redacted]

Building [redacted] is located in a limited access area and accommodates the [redacted] facility.[redacted].

[redacted].

[redacted]. The entrance door is a security door, equipped with a security lock. The windows are equipped with security grills. The rolling door used when the irradiator was installed is now fixed to the concrete by bolts.

[redacted]

Basis:

NSS14 paragraph 4.11 – Detection measures should be implemented for the discovery and assessment of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of radioactive material.

Recommendation 9:

ANSTO should apply detection measures on potential adversary routes into the ——— facility by-passing the routes currently covered by detection measures.

———————————————————————————————————————

———————————————————————————————————————.

XX. TRANSPORT

XX.1 Transport of fresh fuel to ANSTO

The transport of fresh fuel assemblies and un-irradiated uranium targets (Category III) takes place three times a year, on average, from Sydney airport to ANSTO. A transport plan for the period of 2011-2013, prepared by ANSTO and approved ASNO was reviewed by the IPPAS team.

The transport plan:

- Identifies the persons concerned with the transport or in case of an emergency
- Identifies the transported material
- Describes the detailed steps of transport operations
- Describes the transport route
- Lists the contingency and emergency instructions
- Describes the instructions to drivers

In addition to the transport plan prepared by ANSTO and approved by ASNO, a detailed plan (i.e. standard tactical plan) describes the actions to be taken by AFP was also available. The plan, prepared and approved within AFP, describes the tasks of the AFP in response to contingency and emergency incidents.

XIX.2 Transport of radiopharmaceuticals from ANSTO

The IPPAS team saw the vehicle used for the transport of radiopharmaceuticals, when it was parked in front of the transport gate of building ———————, and also reviewed an AFP document regarding general transport of radiopharmaceuticals and a specific transport plan for Category 1 (by aggregation) radioactive sources.

The molybdenum/technetium generators are packed individually in boxes and then transported, on road, to inland users as well as to the airport and then overseas. The activity of a molybdenum/technetium generator varies between 50 and 500 GBq per package. The vehicle is equipped with GPS tracking device with duress possibility. ———————

———————. An AFP post instruction document is developed for transports, which describes the tasks of the ANSTO AFP in relation to the start of the transport as well as its monitoring when on route. The document includes actions to be implemented in case of various emergency situations (i.e. fire, break/down of the vehicle, accident, medical emergency, security event), as well as the security briefing to be provided to the driver of the vehicle.

A specific transport security plan was established for transport of Ir-192 (category 1) from ANSTO to the Sydney airport (realized in June, 2013) in three B(U) types containers. The transport time was less than an hour, therefore stops were not planned. The conveyance vehicle was an ANSTO owned and operated van with one ANSTO driver. The van had remote key lock and the rear doors of the van were locked when in transit to prevent removal. Each ——— container was fitted with restraining straps to secure them to pallets within the van. The contact details of those involved in the transport were listed in the security plan. The vehicle was loaded within the ANSTO site where access was restricted for the purposes of the task.

The following security measures were in place:

- Prior to loading, the transport vehicle was inspected by the AFP for evidence of sabotage or potential mechanical failure.
- Loading of the truck took place within the ANSTO Secure perimeter at the ANSTO Health loading dock, which is external to the building.
- An AFP officer was present while the vehicle is loaded.
- The rear doors of the vehicle were secured for the duration of the transport.
- A GPS remote tracking device accompanied the vehicle and will be monitored in real time by the AFP.
- The driver was briefed by the AFP on the security requirements and emergency procedures prior to departure as outlined in this plan.
- Specific timings and route information will be handled and communicated in accordance with the ANSTO Security Manual on a need-to-know basis as outlined in this plan.

The transport will be direct to the airport with no other goods on board. Travel time to the airport is estimated to be 50 minutes with no scheduled stops. The transport security plan includes actions to be implemented in case of various emergency situations (i.e. fire, break/down of the vehicle, accident, medical emergency, security event) as well as the security briefing to be provided to the driver of the vehicle. This security plan is classified For Official Use Only. It must be kept in a locked cabinet and only made available to persons with an established need-to know. The primary means of communication between all parties involved in transporting the source will be by ANSTO issued mobile telephone and a secondary mobile phone if required. The plan also described the actions to be taken in the event of a change in threat level.

Suggestions (Based on NSS 9) 24:

ANSTO should consider updating the transport security plan to include the following stipulations:

- *Warning signs to be placed on the transport vehicle (for deterrence)*
- *Detailed drawing of the transport vehicle and the cargo within*
- *Each crew member of the conveyance should carry means of positive identification during transport.*
- *Training requirements of staff participating the transport should be specified and tested prior to the commencement of the transport*
- *Physical protection arrangements to be taken in the case of an unexpected extended stop of the transport*
- *The transport vehicle should be equipped with a detection system of attempt of unauthorized removal.*
- *The transport vehicle should be equipped with a remote disabling device in the event the vehicle is stolen or hijacked.*

ACKNOWLEDGEMENTS

The Australian Government provided valuable support to the IPPAS mission, and the advance information provided to team members was of considerable assistance. Key members of ASNO, ANSTO and ARPANSA were most helpful throughout the team's tour by providing insight into the facility's operation, implementation of physical protection measures and the organization of the security guard force and its arrangements for off-site armed response.

Members of the IPPAS team wish to express their appreciation to the numerous officials of who contributed to the success of the mission. The team were privileged to meet with the many professionals who freely offered their expertise and time. All the personnel with whom the IPPAS team had contact were extremely helpful. Their cooperation was instrumental in maintaining a professional and productive atmosphere throughout the course of the mission. The exchange of information regarding international physical protection practice was most beneficial to all parties.

Appendix I: Synopsis of Recommendations, Suggestions and Good Practices

Government Organization, Assignment of Responsibilities and International Obligations

Good practice 1:

Australia, in addition to being involved in all relevant international nuclear security legal (or soft-law) instruments, plays a leading role in a number of international and regional outreach activities aimed at strengthening international nuclear security regime, whereby it intensely exchanges information both directly and through the IAEA and other relevant international organisations.

Recommendation 1:

The Australian Government should introduce a requirement for a regular review and update of the physical protection regime.

National Physical Protection Regime

Recommendation 2:

The Australian Government should review its legislation to ensure that there are no situations where an offender is exempt from sanctions. The review should also bear in mind the absence of administrative offences for less serious breaches of the legislative requirements.

Suggestion 1:

All relevant Australian authorities should complete enabling mechanisms to formalize the process for a designated entity to assume prime responsibility for security in the absence of "authorized persons".

Suggestion 2:

The Australian Government should consider making a formalised arrangement specifying pertinent requirements applicable across the country that would ensure clearer uniformity and predictability of regulation.

Recommendation 3:

The Australian Government should promulgate nuclear security requirements in regulations.

Role & Responsibilities of Competent Authority - ASNO

Suggestion 3:

It is suggested that the staffing level of the regulator be examined to determine the appropriateness of the current staffing level for security responsibilities.

Recommendation 4:

The Australian Government should define the URC or provide formal guidance on the bounding conditions that should be used to determine adequacy of protection to potential sabotage targets.

Suggestion 4:

The Australian Government should consider defining a procedure for establishing the level for high radiological consequences as per NSS 13.

Recommendation 5:

The Australian Government should extend national plans for locating, recovering and assuming control of material out of regulatory control at the border. Further it should define the roles and responsibilities of appropriate state response organizations to locate and recover any missing or stolen material.

Role & Responsibilities of Competent Authority - ARPANSA

Recommendation 6:

The Australian Government should develop security requirements for unsealed sources and wastes in harmony with the requirements established in IAEA NSS No.14.

Suggestion 5:

The Australian Government should consider developing clear requirements for material that is both radioactive and nuclear at the same time.

Suggestion 6:

ARPANSA should consider reformulating the general requirement for security of radioactive sources in the Code of Practice to reflect requirements for sufficient delay after detection to allow effective response.

Suggestion 7:

ARPANSA should consider taking appropriate steps to retain the regulatory role delegated to it by the ARPANS Act.

Suggestion 8:

The maximum licensed activity should provide basis for both safety and security arrangements.

Suggestion 9:

ARPANSA should consider continuing its efforts to include all radioactive sealed sources having activity above the D value into the national register, and provide ability to track the transfer of sources between jurisdictions as well as between jurisdiction and Commonwealth-source users.

Suggestion 10:

ARPANSA should consider providing the same authority to security advisors to conduct inspections on the compliance with security related requirements. At the same time, in order to benefit from safety-security synergy and optimize human resources, ARPANSA should consider training inspectors to have sufficient expertise on both safety and security areas.

Integration & Participation of Other Organizations

Good practice 2:

The Australian Government has established and maintains a security hotline where anyone can report any potential security events.

Suggestion 11:

The Australian Government should consider producing a classification guide that is more specific and relevant to nuclear and radiological issues.

Recommendation 7:

The Australian Government should ensure a uniform approach to information security for all regulated licensees/permit holders.

Threat Assessment & Design Basis Threat

Suggestion 12:

The Australian Government should consider including ——————————— threats as part of its DBT.

Suggestion 13:

The Australian Government should consider a more regular review of the DBT to take into account the changing threat environment.

Risk-Based Physical Protection

Suggestion 14:

ANSTO should consider applying the principle of balanced protection in the design of its physical protection system according to IAEA TECDOC-1276.

Facility Implementation of Physical Protection System at ANSTO

Good practice 3:

ANSTO conducted an on-line nuclear security culture survey to assess the level of the security culture within the organization in 2011. Based on outcomes of the survey ANSTO identified the areas needing further development to reach a more effective nuclear security. As a result of the measures introduced (i.e. security culture change programme) and the continuous endeavour of the security staff for higher effectiveness demonstrated significant improvement in security culture areas during the repeated survey conducted a year later.

Suggestion 15:

ANSTO should consider integrating the different security related plans into one security plan that will include sections dealing with the design, evaluation, implementation and maintenance of the physical protection system, and contingency plans.

Suggestion 16:

ANSTO should consider requesting that ASD conduct a vulnerability assessment (penetration test) to ensure that unauthorised access between ——————————————— network cannot be achieved. The subsequent report should then form part of the security documentation and inform future network alterations.

Suggestion 17:

ANSTO should consider formally re-evaluating the classification of ———————— in accordance with NSS 13, NSS 17, and PSPF Mandatory requirements INFOSEC 3 and PHYSEC 6, to ensure that they have been correctly classified commensurate with the confidentiality, integrity and availability of the data processed, and the Impact Level for each system on the networks. If this results in an increase to the existing residual risk, the network architecture and current security measures (physical, technical, personnel and procedural) should be reviewed to ensure they remain adequate.

Suggestion 18:

ANSTO should consider improving control of access to the ———————— to employ two-factor authentication (i.e. proximity and PIN) at all times.

Good practice 4:

Good practices were noted for the removal of computer equipment offsite, including the use of gate passes and hard drive encryption. All staff, contractors and visitors are required, on entry, to register and seek approval to remove any assets from the facility.

Good practice 5:

ANSTO has implemented an insider threat mitigation strategy. The strategy sets out a broad range of activities designed to mitigate the insider threat risk, including a comprehensive vetting process, which includes five key personnel security elements (honesty, maturity, loyalty, tolerance and trustworthiness).

On-Site & Off-Site Response

Suggestion 19:

ANSTO should consider establishing a process for the independent verification of guard force performance.

Good practice 6:

The effectiveness of on-site response forces for the research reactor is regularly tested by multi-agency force-on-force exercises.

Site Control Centre

Suggestion 20:

ANSTO should consider the appropriateness of current staffing levels of the SCC.

Good practice 7:

Liberal use of flap sheets – laminated instructions containing the actions to be taken in the event of certain incidents. This negates the requirement for AFP personnel to trawl through larger documents when response timings may be critical to success or failure.

Out of Fence, Fence to Buildings

Suggestion 21:

ANSTO should consider prioritising the programming of detection analytics for building —.

Good practice 8:

The principle of long range detection was observed through the use of technology, which far exceeded the protected area boundary.

OPAL

Suggestion 22:
ANSTO should consider improving the effectiveness of access and egress control with respect to unauthorised object detection capability for protected areas.

Building —

Suggestion 23:

Building — would benefit from external CCTV in order to verify any alarms triggered by unauthorized access.

Building —

Recommendation 8:

ANSTO should apply detection measures on potential adversary routes into the radiopharmaceutical production facility by-passing the routes currently covered by detection measures.

Building —

Recommendation 9:

ANSTO should apply detection measures on potential adversary routes into the —— facility by-passing the routes currently covered by detection measures.

Transport

Suggestion 24:

ANSTO should consider updating the transport security plan to include the following stipulations:

- *Warning signs to be placed on the transport vehicle (for deterrence)*
- *Detailed drawing of the transport vehicle and the cargo within*
- *Each crew member of the conveyance should carry means of positive identification during transport.*
- *Training requirements of staff participating the transport should be specified and tested prior to the commencement of the transport*

- *Physical protection arrangements to be taken in the case of an unexpected extended stop of the transport*
- *The transport vehicle should be equipped with a detection system of attempt of unauthorized removal.*
- *The transport vehicle should be equipped with a remote disabling device in the event the vehicle is stolen or hijacked.*

Appendix II: IPPAS Team Composition

Kristof Horváth, Hungary	(team leader)
———, Czech Republic	(legal expert)
——————, Republic of Korea	(physical protection expert)
——————, UK	(cyber security expert)
——————, Canada	(regulatory expert)
———, Indonesia	(physical protection expert)
——————, IAEA	(mission coordinator and physical protection expert)