INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

Follow-up Mission Report: Australia

30 October - 10 November 2017

Prepared for the Government of Australia

ABBREVIATIONS

ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
ANM	ANSTO Nuclear Medicine
ANSTO	Australians Nuclear Science and Technology Organisation
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ASIO	Australian Security Intelligence Organisation
ASNO	Australian Safeguards and Non-Proliferation Office
ASOC	ANSTO Security Operations Centre
ASQA	Australian Skills Quality Authority
AV	Anti-Virus
BMS	Balanced Magnetic Switch
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CIO	Chief Information Officer
CoC	Code of Conduct on the Safety and Security of Radioactive Sources
CPPNM	*Convention on the Physical Protection of Nuclear Material* (INFCIRC/274/Rev.1)
DBT	Design Basis Threat
DFAT	Department of Foreign Affairs and Trade
DLM	Dissemination Limiting Marker
DU	Depleted Uranium
EACS	Electronic Access Control System
EPR	Emergency Preparedness and Response
ERM	Enterprise Risk Management
GICNT	Global Initiative to Combat Nuclear Terrorism
HEU	High Enriched Uranium
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICT	Information and Communications Technology
ID	Identification
IDS	Instruction Detection System
INFCIRC	Information Circular

IPPAS	International Physical Protection Advisory Service
IRAP	Information Security Registered Assessors Program
ISM	Information Security Manual
ITDB	Incident and Trafficking Database
ITSA	Information Technology Security Advisor
KMP	Key Measurement Points
KPI	Key Performance Indicators
LAD	Licence Administration Database
LEU	Low Enriched Uranium
LMS	Learning Management System
LOF	Locations Outside Facilities
MAC	Media Access Control
MBA	Material Balance Area
MoU	Memorandum of Understanding
NMAC	Nuclear Material Accounting and Control
NSS	IAEA Nuclear Security Series
NSSR	National Sealed Source Register
OPAL	Open Pool Australian Lightwater research reactor
PCSS	People Culture Safety and Security
PIR	Passive Infrared Sensor
PIV	Physical Inventory Verification
PPS	Physical Protection System
PSPF	Protective Security Policy Framework
PSR	Periodic Safety Review
PSSR	Public Safety and Security Review
PTZ	Pan-Tilt-Zoom
QCVS	Quality Control Verification System
RAR	Regulatory Assessment Report
RCMS	Reactor Control Management System
SCEC	Security Construction Equipment Committee
SSAC	State Systems of Accountancy and Control
SSOC	Security and Safeguard Oversight Committee
UPC	Uninterruptable Power Supply
URC	Unacceptable Radiological Consequent
VPN	Virtual Private Network

VRF	Virtual Routing and Forwarding
WINS	World Institute for Nuclear Security

CONTENTS

SUMMARY

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) Follow-up mission conducted in Australia from 30 October - 10 November, 2017. This is the 80th IPPAS mission conducted by the IAEA since the introduction of this service in 1995. Australia hosted an initial IPPAS mission in 2013.

The objectives of the IPPAS mission were to make an assessment of the Australian Commonwealth level nuclear security regime and the facility level physical protection systems and measures at Australian Nuclear Science and Technology Organisation (ANSTO), as computer security and nuclear material accounting and control, and to compare the procedures and practices in Australia with the CPPNM and its 2005 Amendment, Code of Conduct of Safety and Security of Radioactive Sources, the IAEA Nuclear Security Series recommendations No. 13 (INFCIRC/225/Rev.5), No. 14, and other NSS guidance documents.

The scope of the two-week International Physical Protection Advisory Service (IPPAS) follow-up mission included responses to the recommendations and suggestions of the initial mission conducted in 2013, any changes in the Commonwealth legislative and regulatory framework for nuclear security since 2013, computer security and nuclear material accounting and control. Australia's implementation of the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) was also confirmed.

The IPPAS team visited the Lucas Height Campus of ANSTO, including the Open Pool Australian Light water (OPAL) Research Reactor and the newly established ANSTO Nuclear Medicine facility (ANM).

For this IPPAS mission, the IAEA assembled a seven-person team comprising experts from five Member States and the IAEA. The experts have broad expertise and experience in nuclear legislation, regulatory oversight, physical protection system design, implementation and assessment, including computer security and nuclear material accounting and control. During the mission, the IPPAS team interacted with key management and personnel from the Australian Safeguards and Non-Proliferation Office (ASNO), the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), the Australian Cyber Security Centre, the Australian Federal Police (AFP), as well as the management and staff from ANSTO.

It was apparent to the IPPAS team that a significant amount of time and effort was invested by ASNO, ARPANSA and ANSTO in the preparation and conduct of the mission. The Australian host organisations provided the IAEA and the IPPAS team members with an advanced information package consisting of relevant information related to Australia's legislative and regulatory framework, roles and responsibilities of the competent authorities and other Australian organisations involved in nuclear security, as well as information on nuclear and other radioactive material, associated facilities and activities. The relevant Australian legal and regulatory documents on nuclear security were also included in the advance information package.

The IPPAS team observed that the nuclear security regime in Australia is well established and incorporates the fundamental principles of the amended CPPNM.

It is important to note that Australia is adhering and contributing to all international instruments relevant to nuclear security and that Australia's nuclear security legislation is continually being updated and enhanced. The IPPAS team also noted that both ASNO and ARPANSA encourage the adoption of good nuclear security practices.

A total of five good practices were identified during the mission, which if shared, could benefit other Member States in enhancing nuclear security. The first good practice recognized encompassing nuclear security within the periodic safety review process. Two good practices supported insider threat mitigation measures recognizing the value of the "no alone zone" function of the Electronic Access Control System, and operational process overview of the ANM facility. The final two good practices are related to computer security related activities.

The IPPAS team provided recommendations and suggestions to support Australia in enhancing and sustaining nuclear security.

There are a total of four recommendations that were made during the IPPAS Mission. The first related to the requirement to establish a national register of radioactive sources. Three other recommendations are made to strengthen computer security measures and their oversight.

There are a total of fifteen suggestions that were made during the IPPAS Mission. There were two suggestions related to staff level reviews, one suggestion related to ASNO and ARPANSA joint guidance on the application of the threshold for unacceptable radiological consequences, six suggestions on cyber security, one related to search process at ANSTO, two related to system performance, one regarding nuclear material accounting and control activities, one related to correlating Commonwealth Government standards to IAEA NSS 13 & 14 recommendations and guidance, and one suggestion relating to a management action plan to address IPPAS outcomes.

The IPPAS team noted that considerable effort has been undertaken by ASNO, ARPANSA and ANSTO to address Recommendations and Suggestions arising from the 2013 IPPAS Mission report. The IPPAS team assesses that this effort will serve to strengthen Australia's nuclear security regime.

It is noted however that some effort to address Recommendations and Suggestions remains a work in progress. The IPPAS team encourages expedited and continued efforts to address these issues in a timely fashion to the extent possible while recognizing the challenges of achieving resolutions are sometimes cumbersome and complicated.

In conclusion, the IPPAS team assesses that Australia has a mature and well-established nuclear security regime, which has been enhanced significantly in the recent decade and further on the basis of the 2013 IPPAS mission report.

The mission report is treated by the IAEA as "Highly Confidential" and protected accordingly. Distribution of the IPPAS mission report is at the discretion of the Government of Australia. The IAEA will make the report available for third parties only with the express permission of the Government of Australia.

I. INTRODUCTION

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) Follow-up mission conducted at the request of the Government of Australia.

On 29 July, 2015, the Australian Department of Foreign Affairs and Trade requested that the IAEA arrange an IPPAS follow-up mission to reassess Australia's nuclear security regime. The IAEA agreed to conduct the mission from 29 October to 10 November, 2017.

I.1 Objectives

The objectives of the IPPAS mission were to make an assessment of the Australian Commonwealth level nuclear security regime and the facility level physical protection systems and measures at Australian Nuclear Science and Technology Organisation (ANSTO), as well as computer security and nuclear material accounting and control, and to compare the procedures and practices in Australia with the CPPNM and its 2005 Amendment, Code of Conduct of Safety and Security of Radioactive Sources, the IAEA Nuclear Security Series recommendations No. 13 (INFCIRC/225/Rev.5), No. 14, and other NSS guidance documents.

The team gathered information on the current legal and regulatory framework through presentations and interviews with officials representing the competent authorities of Australia. The IPPAS team visited and observed the facility level implementation of physical protection systems and measures at the Lucas Heights Campus of ANSTO, including the Open Pool Australian Ligthwater (OPAL) Research Reactor and the newly established ANSTO Nuclear Medicine (ANM) facility.

Meetings with staff of competent authorities and ANSTO, as well as the facility visits provided opportunities for 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.

I.2 Scope

The scope of the two-week International Physical Protection Advisory Service (IPPAS) follow-up mission included responses to the recommendations and suggestions of the initial mission conducted in 2013, any changes in the commonwealth legislative and regulatory framework for nuclear security since 2013, computer security and nuclear material accounting and control. Australia's implementation of the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) was also confirmed.

The National Review (Module 1) focused on the changes in the national physical protection regime of nuclear material and nuclear facilities including the Australian Security and Non-Proliferation Office (ASNO).

The Nuclear Facility Review (Module 2) focused on the changes in the physical protection measures of the OPAL research reactor facility and Building ———— Facility operated by ANSTO.

The Radioactive Material Security Review (Module 4) focused on the security regime of other radioactive materials, including Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), and the ANSTO Nuclear Medicine (ANM) facility. Taking account that the ANM facility is a nuclear facility, which also uses and stores other radioactive material; and, in order to prevent

repetition, the report includes the radioactive material security related assessment of the ANM facility in a consolidated manner under Modules 2&4.

The Computer Security Review (Module 5) focused on the computer security measures implemented at Commonwealth level by the Australian Cyber Security Centre and on facility level by ANSTO.

Nuclear Material Accounting and Control (Pilot Module) focused on how the State System of Accountancy and Control (SSAC) and the facility level Nuclear Material Accounting and Control (NMAC) support nuclear security.

The responses provided by the ASNO, ARPANSA and ANSTO regarding the considerations and measures made in relation to the recommendations and suggestions provided by the IPPAS Mission in 2013, together with evaluation by the IPPAS team are also included in this report.

NATIONAL REVIEW OF NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL (MODULE 1)

II. GOVERNMENT ORGANIZATIONS, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION

The 2013 IPPAS mission report for Australia provides a complete description of these issues. This follow-up mission is focused on changes made since the previous IPPAS mission. In general, minor changes were observed at this level in the past four years.

Security, Safeguards and Safety are the responsibility of two government organizations: the Australian Safeguards and Non-Proliferation Office (ASNO) and the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). ASNO is responsible for safeguards and nuclear security. ARPANSA is responsible for the regulation of radioactive materials and nuclear safety. The two agencies work closely together to ensure that all aspects for safety, security and safeguards are adequately addressed.

II.1 International Obligations and International Cooperation

Australia is a party to all relevant international agreements related to the nuclear field covering areas of nuclear security, non-proliferation, emergency preparedness, waste management and nuclear facilities as described in the 2013 IPPAS report.

Australia continues to play a major role in encouraging the global community to develop appropriate measures and systems to strengthen nuclear security measures. It continues strong support to the IAEA in the field of nuclear security through commitments of financial and technical support and active participation in a number of advisory groups, committees and assisting in the development of nuclear security guidance publications. Australia participated actively in the Nuclear Security Summits and sponsored gift baskets in support of the Summits. Australia continues its strong contributions in the area of nuclear forensics.

Australia further demonstrates this commitment through provision of expert staff to act as team members and team leaders to other IPPAS missions and other peer review mechanisms. Australia was a founding member and actively participates in Global Initiatives to Combat Nuclear Terrorism (GICNT) activities including hosting exercises and leading international outreach and capacity building sessions. It is particularly engaged in regional capacity building where it plays a leadership role as evidenced through its GICNT activities.

III. LEGISLATIVE AND REGULATORY FRAMEWORK

III.1 Primary and secondary legislation

Only minor changes were observed by the IPPAS team in this area since 2013.

III.2 Technical Guidance and Instruments

The Department of Foreign Affairs and Trade (DFAT) to which ASNO staff are employed, published a Guide for Better Risk Management. This guide documents how risk is to be managed within DFAT. ASNO is in the process of developing a related guide to document how risk is managed within ASNO.

ASNO is in the process of developing a Classification Guide for Safeguards and Security Information Relating to Nuclear Facilities, Nuclear Material and Associated Items. This guide will better enable the identification of the level of protection required for information and information systems.

ASNO has begun the process of developing generic templates for permits. They have grouped their permit holders up into 20 classes of users. For each of these user classes, they have created a generic template/model for the permit. Collectively, these templates contain the following information:

- Permit Holder Specific Details,
    - Name and Address,
    - Expiry Date,
    - Definitions,
    - Maximum nuclear material limits,
    - Approved Locations,
    - Approved Uses,
- High-level principles,
    - Security Plan,
    - Accountancy and Control Plan,
    - Records and Reporting,
    - ASNO and IAEA Inspections,
- Detailed Regulatory Requirements,
    - Objectives,
    - Management,
    - Plans and Procedures,
    - Accountancy Requirements,
    - Security Requirements,
        - Threat, Vulnerability and Risk,
        - Security System,
        - Information Security,
        - Personnel Security,
        - Guarding and Response,
        - Interfaces (Safety and NMAC),

- Compensatory Measures,
- Etc.

The IPPAS team conducted a high level review of the content of the S1 permit and confirmed that the permit is consistent with the requirements recommended in IAEA NSS 13.

These generic permits, including the compliance codes, will be published on-line to allow for greater transparency and enable stakeholders to better understand the specific security requirements for the range of facilities that exist in Australia.

ASNO developed a draft procedure on how to conduct a minor review of the Australian National Design Basis Threat. The design basis threat was updated in 2017.

In June 2017 ARPANSA published revised regulatory guidance on holistic safety which forms the basis for an integrated safety and security management. The Periodic Safety and Security Review (PSSR) has become an (ARAPNSA) license and an (ASNO) permit condition for the OPAL reactor at ANSTO and is due in 2019. Previously, nuclear security had not been addressed in the ANSTO Periodic Safety Review (PSR) but instead was addressed separate in the license condition LC14. With the publication of the joint ARPANSA/ANSTO regulatory guide on periodic safety and security review of research reactors in 2016 all important aspects of safety and security will be covered in one comprehensive evaluation.

Currently, the international guidance documents do not specifically recommend an integrated PSSR. But because of the interdependency between safety and security it is seen as beneficial to conduct these comprehensive reviews collectively in a global assessment.

Good Practice 1 (2017): The regulatory body encompasses nuclear security within the Periodic Safety Review process of a research reactor, integrating nuclear safety and security in prioritization of the improvement measures assuring the future safe and secure operation of the facility.

The IPPAS team was informed that ARPANSA and ASNO have established thresholds for URC and HRC according to Recommendation 4 and Suggestion 4 of the IPPAS 2013 report. Guidance on appropriate application of these thresholds does not exist currently.

Suggestion 1 (2017): ASNO and ARPANSA should consider providing joint guidance on the appropriate application of URC and HRC for the license holders.

IV. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY (ASNO)

ASNO's role and responsibilities has not changed in the last four years.

V. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)

ASNO developed a draft procedure on how to conduct a minor review of the Australian National Design Basis Threat. This procedure guides ASNO staff in conducting periodic minor reviews every 12-24 months.

As a result of the most recent minor review in 2017, the design basis threat was updated.

VI. SUSTAINING THE PHYSICAL PROTECTION REGIME

VI.1 Staffing

Supplementing the information provided in the 2013 IPPAS mission report and the responses to recommendations and suggestions resulting from that report, the IPPAS team noted that ASNO's Nuclear Security Section staff has been augmented as described below.

ASNO advised the IPPAS team that it has increased its staff by one full time equivalent staff member to manage "regulatory systems" These functions include activities related to:

- Establishing a Quality Management System,
- Ensuring knowledge management,
- Formalising risk management.

This staff member provides assistance, among other duties, quality management functions to the ASNO Security Section.

The IPPAS team recognised that some of the resource-intensive international commitments, such as the Nuclear Security Summits have been reduced. The IPPAS team noted however that the breadth of staff and experience may be insufficient to perform timely detailed technical analysis associated with reviews of PSRs, adversary pathway and delay value analysis etc. Since the thresholds for Unacceptable Radiological Consequences (URC) and High Radiological Consequences (HRC) are now defined, additional detailed review and assessment by ASNO will be required to evaluate permit holders submissions associated with vital area candidate assessments.

Suggestion 2 (2017): ASNO should consider performing a systematic staffing review of its Security Section to confirm adequacy of staffing to perform the current and emerging tasks through mapping all necessary tasks, including cyber security, against resources.

VI.2 Directive on the Security of Government Business

The Australian Government takes appropriate measures to protect its people, information and assets, at home and overseas. "How the Government protects its people, information and assets is critical to effective engagement with the Australian people. The Protective Security Policy Framework (PSPF) is designed to help agencies:

- identify their levels of security risk tolerance,
- achieve the mandatory requirements for protective security expected by Government, and develop an appropriate security culture ..."

VII. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

No significant changes were observed in this area since 2013.

The IPPAS team welcomed the on-going security exercises conducted at Commonwealth level to confirm the effectiveness of the current arrangements.

NUCLEAR FACILITY REVIEW
(MODULE 2)

VIII. AUSTRALIAN NUCLEAR SCIENCE AND TECHNOLOGY ORGANISATION (ANSTO)

– This chapter has been omitted –

.

NUCLEAR FACILITY REVIEW AND SECURITY OF RADIOACTIVE MATERIAL AND ASSOCIATED FACILITY REVIEW (MODULE 2&4)

– This chapter has been omitted –

SECURITY OF RADIOACTIVE MATERIAL (MODULE 4)

Safety, Security and Safeguards are the responsibility of two government organizations: ARPANSA and ASNO. In general, ARPANSA is responsible for the regulation of radioactive materials and nuclear safety. ASNO is responsible for safeguards and nuclear security. The two agencies work closely together to ensure that all aspects for safety, security and safeguards are adequately addressed.

IX. LEGISLATIVE AND REGULATORY FRAMEWORK

IX.1 Primary legislation

The Australian Radiation Protection and Nuclear Safety Act of 1998 ("ARPANS Act") was amended in 2015 and the changes came into effect on 8 October 2015.

The Minister of Health, by Administrative Order, administers the ARPANS Act. The ARPANS Act focuses primarily on radiation protection as stipulated in its Section 3. The fundamental objective is to protect the health and safety of the people, and to protect the environment from the harmful effects of radiation. Australian Radiation Protection and Nuclear Safety Regulations are issued to implement the ARPANS Act. The Act was amended once and the Regulations were amended annually since the last IPPAS in 2013.

The Act applies to controlled persons; the definition of controlled persons does not cover natural or legal persons that are licensed or regulated by the State or territory governments.

ARPANSA issues license to controlled persons to undertake certain activities in relation to controlled facilities such as research reactor, controlled apparatus (X-ray machines) and controlled material (radioactive sources). Relevant changes to the Australian Radiation Protection and Nuclear Safety Act 1998 and Regulations 1999 are as follows:

- A license can now be issued for a fixed period; previously license was valid until cancelled or surrendered flexibility is provided to the CEO of ARPANSA to restrict duration of a license;
- CEO of ARPANSA is enabled to direct the license holder to do or not to do something if there's a risk of death and serious injury or serious damage to the environment; previously the CEO of ARPANSA was enabled to direct only in the case of non-compliance with the ARPANS Act or Regulation.

IX.2 Secondary Legislation

Regulation 49 was amended in 2015 as follows: license holders must have in place plans and arrangements that include security plan and emergency plan, and must take steps to implement the plans and arrangements. These plans and arrangements will be reviewed at least once every 3 years, to review and update any plans and arrangement for managing the controlled facility, controlled material or controlled apparatus to ensure the health and safety of people and protection of the environment. The CEO of ARPANSA will issue a license, taking into account the advice provided by the regulatory

officers contained in the Regulatory Assessment Report (RAR), international best practice and other information (ARPANSA codes and standards of particular relevance). License applicants are required to demonstrate compliance with RPS-11 (Security of Radioactive Sources) and the security requirements in the Regulatory Guide "Plans and Arrangements for Managing Safety" in order to gain or retain the license.

The IPPAS team noted Radiation Protection Series Publication No. 11 (RPS-11) Security of Radioactive Sources still does not apply to unsealed radioactive sources and radioactive waste. The IPPAS team was informed that ARPANSA would wait the publication of the revised IAEA NSS No. 11 where unsealed sources and radioactive waste are included in the security requirements.

IX.3 Technical Guidance

Regulatory Guide "Holistic Safety" promotes an integrated management approach for safety, security and emergency preparedness; however, it is not mandatory.

The Regulatory Guide "Plans and Arrangements for Managing Safety" is applicable to both sources and facilities and should be used during the preparation of the license application. The approach provides flexibility to the license holders in preparation of the license application.

ARPANSA advised the IPPAS team that it has implemented the process whereby accredited assessors can assess and endorse security plans for approval by the state or territory regulator. Accredited Assessors are required to successfully undertake a certificate program course. The course is intended to provide participants with the skills and knowledge to perform the role of Radiation Security Advisor. Upon successful completion of the course, they may apply for accreditation. The Security Advisors are accredited by the Australian Skills Quality Authority (ASQA).

X. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY (ARPANSA)

X.1 Inspector Training Programme

ARPANSA has developed an inspector training programme, which contains 11 separate modules that all ARPNSA inspector candidates must successfully complete before issuance of an inspector certification (i.e. inspector card). The training programme integrates training for safety, security and emergency preparedness and response in order to provide a comprehensive inspector knowledge which is then augmented with "core speciality training".

The programme has not been identified as a mandatory requirement for those inspectors already holding an inspector card as implementation of the training is ongoing. Assessment of training needs for previously certified inspectors has yet to be undertaken.

X.2 National Register of Sealed Sources

During the course of discussions with ARPANSA staff, the IPPAS team was informed that the National Sealed Source Register as described in the previous 2013 IPPAS Report is no longer in existence. It was provided that:

"In 20l6, through the Radiation Health Committee (all regulators), members agreed to abandon the National Sealed Source Register (NSSR) and replace this with a Network of National Registers which can be called upon by contacting the relevant jurisdictional radiation regulator at any time. This approach acknowledged that the complexity of operating a system which accesses nine (9) different database systems was technically and commercially challenging, and heeded the Australian Government policy which expects an 'enter once, use multiple times' approach to managing data. Some regulators were manually extracting and entering data into the NSSR, as automation was not feasible due to resources. ARPANSA retains a record of all imports and all high activity exports entering and exiting the country. ARPANSA retains all sources held by Commonwealth licence holders through our Licence Administration Database (LAD). ARPANSA can call upon any jurisdiction to gain source data at any time, and has done so during investigations in recent times. The results have included actual prosecutions. ARPANSA believes this system is working well."

The IPPAS team noted that this decentralized process does not assure uniformity of registering and reporting the transfers of radioactive sources in the Commonwealth, State and Territory levels. It was determined that the system has not been performance tested to confirm accuracy, completeness and timely informing. The IPPAS team evaluated that this arrangement does not align to the expectations of the Code of Conduct.

Basis: Code of Conduct on the Safety and Security of Radioactive Sources Basic Principles, Paragraph 11 which provides that *"each State should establish a national register of radioactive sources..."*

Recommendation 1 (2017): The State should establish a national register of radioactive sources.

COMPUTER SECURITY REVIEW (MODULE 5)

XI. STATE LEVEL REVIEW

XI.1 Legal and Regulatory Framework

The Australian Government has several organizations at the Commonwealth level with responsibilities for security protections of nuclear facilities and material to govern and provide regulation, policy and guidance for computer security. For cyber security protections, the following three organizations provide governance:

- Australian Radiation Protection and Nuclear Safety Agency (ARPANSA),
- Australian Safeguards and Non-Proliferation Office (ASNO),
- Australian Signal Directorate (ASD).

Each of these organizations above play a critical role in the guidance and protection of Information and Communications Technology (ICT) for nuclear facilities. ASNO has developed a State Level DBT that has designed out the "beyond the DBT". This has been done in partnership with other competent authorities and ANSTO, where they have built in the coordination with the competent authorities and the State to address any DBT. The Attorney General's Department is responsible for the overarching protective security policy framework, ASIO for Australia's security, and CERT for CNI including industrial control systems. Threat information is also reviewed and analysed by ASD, and information is directly shared down to ASNO and licensees.

ASD advises agencies such as ANSTO on their own incident response. ASD can deploy an incident response team to assist government with compromised systems. They are able to assist in identifying an infection, containing the environment, eradicating the malware and restoring the system(s) back to full operations. ASD also provides a service for monitoring Commonwealth networks through sensors on external gateways (firewalls) for early notifications. Currently, ASD's present focus is to provide these services to Commonwealth Government organisations. The Australian Government 2017 Independent Intelligence Review recommended legislative change to extend ASD's mandate to include providing advice to the private sector. Legislative changes are expected in the second half of 2018.

Under the PSPF, ASD has two categories of compliance, 'must', and 'should' based on the degree of security risk an agency would be accepting by not implementing the control. ASD, under the ACSC, has the 'Essential Eight', out of which the Top 4 mandatory requirements to implement include:

- application whitelisting,
- patch applications,
- restricting administrative privileges, and
- patch operating systems.

ASD recommends and promotes the 'Essential Eight' for all organisations as the baseline for cyber security.

Some of the current controls for government systems cannot be directly applied to industrial controls systems and the ICT networks that support critical operations. One specific example is application whitelisting. Accordingly, specific care needs to be taken to make sure all applications within industrial control systems including life safety element, which never operates until a specific event is triggered. A review of relevant controls and their applicability to industrial control systems should be undertaken by ASD once it has a legislative mandate to engage the private sector.

Basis: IAEA NSS 17, Paragraph 2.3 Site Security Framework states, *"All disciplines of security (including personnel, physical, information and computer) interact and complement each other to establish a facility's security posture as may be defined in the SSP. A failure in any of the disciplines of security could impact the other domains and cause extra requirements on the remaining aspects of security. Computer security is cross-cutting discipline that has interactions with all other areas of security in a nuclear facility".*

Suggestion 8 (2017): The relevant Competent Authority should consider providing cyber security advice on industrial control systems for Australia's critical national infrastructure, should consider advising ANSTO and other relevant entities to develop specific requirements for industrial control systems so that recommended security requirements, best practices, and guidance do not negatively impact safe and secure operations.

ARPANSA provides core services for Source Control, Facility Licensing, Continuous Improvements, and Regulator Assurance. The key element for ICT security is within the Operator's license that authorized a site to operate. Within the licensing framework, there are permits that are issued by ASNO, which define the requirements to be met by the Operator.

The specific Permit of reference is the PERMIT TO POSSESS NUCLEAR MATERIAL & ASSOCIATED ITEMS. This permit is granted pursuant to Section 13 of the *Nuclear Non-Proliferation (Safeguards) Act l987* ("the Act"). The permit requires the licensee to effectively classify and protect security sensitive information in accordance with relevant Australian government standards for protective security and of government ICT. The term Australian government standards is further defined as: "In the context of this Compliance Code means the Australian Government Protective Security Policy Framework (PSPF) or Order and the Information Security Manual (ISM), as applicable."

The PSPF was developed by the Attorney General's Department to protect people and information assets. Within the PSPF, there are thirty-six mandatory requirements covering Governance, Personnel, Information and Physical security.

ASD maintains the ISM, providing a risk based approach to protecting information and systems. The advice in the manual is specially based on ASD's experience in providing cyber and information security advice and assistance to the Australian government. The controls are therefore designed to mitigate the most likely threats to Australian government agencies.

ARPANSA and ASD did not use IAEA NSS 17 - Computer Security at Nuclear facilities to define their required security control and guidance. ARPANSA has, however, reviewed the IAEA NSS 17 document and adopted it as guidance, and posted it to their website for use, but it is not enforceable. Based on that information, the IPPAS computer security team member did a cross-walk of the IAEA NSS 17 security control requirements with the PSPF and ISM requirements and verified that they are equally represented.

Good Practice 4 (2017): The Competent Authority for cyber security provides guidance to the industry through an Information Security Manual. The Competent Authority has a continuous improvement process to maintain the currency and relevance of the Information Security Manual with the changing landscape of cyber security. The Competent Authority for cyber security

conducts surveys to the industry and, updates the Information Security Manual on a yearly basis, based on feedback and any new threat information.

XI.2 Roles and Responsibilities of Competent Authority

XI.2.1 Australian Signal Directorate (ASD)

ASD is the federal level competent authority on the security of information under the Commonwealth Intelligence Services Act 2001 with a legislative mandate to provide material, advice and assistance to Commonwealth and State entities on cyber security. ASD, through the Australian Cyber Security Centre (ACSC), issues technical standards, international representation, and provides operational governance within the PSPF for all ICT systems. In relation to information and computer security, ACSC:

- analyses threats to critical ICT infrastructure,
- develops shared situational awareness across a broad set of partners and stakeholders,
- leads the national cyber security efforts and the response to cyber incidents.

XI.2.2 Australian Security and Non-Proliferation Office (ASNO)

ASNO is tasked to enhance the Australian and international security through activities which contribute to effective regimes against the proliferation of nuclear and chemical weapons. ASNO performs domestic regulatory functions to ensure that Australia is in compliance with the commitments undertaken in the relevant international treaties and that the public is protected through the application of high standards of safeguards and physical protection to nuclear materials and facilities. In relation to information and computer security, ASNO:

- establishes regulation of the security of nuclear material and facilities and associated items (material, equipment and technology),
- provides Australia's designated point-of-contact for the CPPNM, and
- is the point-of-contact for the IAEA ITDB in relation to nuclear material.

ASNO is the regulator in the field of computer security of nuclear facilities. The current capabilities of ASNO do not enable the effective regulatory oversight in this area. Regulatory oversight is not performed currently.

Basis: IAEA NSS 13 Paragraph 3.20 says that *"The State's competent authority should be responsible for verifying continues compliance with the physical protection regulations and license conditions through regular inspections and for ensuring that corrective action is taken, when needed."*

Recommendation 2 (2017): ASNO should develop capability to ensure effective regulatory oversight in the field of computer security of nuclear facilities.

XI.2.3 Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)

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). ARPANSA's primary role is to assist Agency Heads and Senior Executives through the PSPF to identify their responsibilities to:

- manage security risks to their people, information and assets,

- provide assurance to the government and the public that official resources and information, provided to their entity are safeguarded,
- is the point-of-contact for the IAEA ITDB in relation to radioactive material, and
- incorporate protective security into the culture of their entity.

XI.2.4 Attorney General's Department

The Attorney General's Department sets the Australian Government's protective security policy including:

- accountability, roles and responsibilities, and
- functional and clear procedures.

XII. FACILITY LEVEL REVIEW AT ANSTO

– This chapter has been omitted –

NUCLEAR MATERIAL ACCOUNTING AND CONTROL (PILOT MODULE)

XIII. STATE LEVEL REVIEW

Australia has established a state system of accounting for and control of nuclear material and associated items according to following international treaty and agreements:

- Treaty on the Non-Proliferation of Nuclear Weapons ratified on 23 January 1973;
- Agreement between Australia and the International Atomic Energy Agency for the application of safeguards in connection with the Treaty on the Non-proliferation of Nuclear Weapons, signed on 10 July 1974;
- Protocol Additional to the Agreement between Australia and the International Atomic Energy Agency for the application of safeguards in connection with the Treaty on the Non-proliferation of Nuclear Weapons, signed on 23 September 1997, date of effect in Australia is 10 December 1997.

The table below lists nuclear material in Australia.

CATEGORY	**QUANTITY**			**INTENDED END-USE**
Source Material:	**2017**	**2013**	**Unit**	
Uranium Ore concentrates (UOC)	773	1666	tonnes U	Exports for energy use pursuant to bilateral safeguards
	3.5	6.0	tonnes U	Storage
Natural uranium (other than UOC)	4,487	4,502	kg	Research and shielding
Depleted uranium	26,721	19,492	kg	Research and shielding
Thorium ore residues	59	59	tonnes	
Thorium	1,940	1,952	kg	Research, industry
Special Fissionable Material:				
Uranium-LEU-235	202,836	169,309	grams	Research, industry, radioisotope production

Uranium-HEU-235	2,741	2,741	grams	Research
Uranium-233	3.8	4.0	grams	Research
Plutonium (except Pu-238)	1,203	1,226	grams	Research, neutron sources

The table below lists Australia's former and current IAEA Material Balance Areas and their current status.

MBA	Name	No of KMP	Details and Status
AS-A	HIFAR Reactor	-	No material - Awaiting Decommissioning
AS-B	MOATA Reactor	-	No material - Decommissioned
AS-C	Research and Development Labs	3	^{99}Mo production using LEU targets & storage and a range of other R&D activities.
AS-D	Vault Storage	3	Storage of seldom used material
AS-E	Locations Outside Facilities (LOFs)	- 100	Small holdings of nuclear material held at Universities, Radiographers, Labs etc.
AS-F	OPAL Reactor	4	Open Pool Australian Light-Water (LEU)
AS-G	Silex Systems Limited	-	No material - Decommissioned
AS-H	Synroc Waste Immobilisation plant	-	No material - Not yet constructed

IAEA Safeguards inspections are conducted on regular basis. The table below provides information about the frequency of IAEA Safeguards inspections.

	Inspection type	Features	Frequency in Australia
CSA	Physical inventory verification (PIV)	• Scheduled • Thorough verification of inventory	**ANSTO**: 1 per year **LOFs**: 1 per -4 yrs **Uranium Mines**: none
CSA	Design information verification (DIV)	• Scheduled • Check design features	**ANSTO**: few per year, in conjunction with PIV **LOFs**: none **Uranium Mines**: none

CSA	Random interim inspection (RRI)	• 3 hrs notice • Less intense than PIV	**ANSTO**: 1 per year **LOFs**: none **Uranium Mines**: none
AP	Complementary Acces s (CA)	• 2hr notice (if onsite) • 24hr notice (if offsite)	**ANSTO**: few per year, in conjunction with PIV, RRI **LOFs**: 1 per 1-2yrs **Uranium Mines:** 1 per 1-2 yrs

XIII.1 Legislative and Regulatory Framework

The *Nuclear Non-Proliferation (Safeguards) Act l987* makes provisions in relation to the non-proliferation of nuclear weapons and establishes, in accordance with certain international treaties and agreements to which Australia is a party, a system for the imposition and maintenance of nuclear safeguards in Australia, and for related matters.

The requirement to establish and maintain an effective NMAC programme is included in the Australian legislative and regulatory framework.

Part I, Section 3 of the Safeguards Act provides that the principal object of Safeguards Act is to give effect to certain obligations that Australia has committed to as a party to the Non-Proliferation Treaty, the Safeguards Agreement, the Additional Protocol and the prescribed international agreements.

The functions of Director General of ASNO are set out in the Part IV - Division 1, Section 43 of the Safeguards Act. Among others, functions related to the operation of Australian Safeguards System are:

- to ensure the effective operation of the Australian safeguards system;
- 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;
- to monitor compliance with the provisions of the prescribed international agreements by parties other than Australia;
- to undertake, co-ordinate and facilitate research and development in relation to nuclear safeguards;
- to advise the Minister on matters relating to the operation of the Australian safeguards system.

The Australian Safeguards Office function conducted by ASNO is established according Safeguards Act Division 2, Section 54. The Australian Safeguards Office consists of the Director and the staff. The IPPAS team was informed that the IAEA Safeguards section within ASNO is currently staffed by four persons.

The Safeguards Act establishes a system for control over nuclear material and associated items in Australia through requirements for permits for their possession and transport.

ASNO issues several types of permits for possession of nuclear materials depending on inventory, applying the principle of the graded approach. Types of permits are:

- L - Permit for Locations Outside Facilities (LOFs) (mainly universities and small laboratories),

- R - Radiographer permits (DU),
- S - Special permits (e.g. ANSTO),
- U - Uranium mines, ports, UOC Agents.

Basic NMAC conditions common to LOF permits are:

- Keep accurate and up-to-date records of inventory and inventory changes,
- Ensure quantities remain within permit limits,
- Do an annual inventory taking,
- Provide annual report to ASNO of all inventory and all inventory changes in last year,
- Provide annual report of descriptions of relevant buildings (AP 2.a.iii),
- Apply appropriate security,
- Allow ASNO and IAEA inspections.

There are a several types for LOF permits depending of element and isotope weight (L1, L2 and L3).

There are two types of radiographer permits depending on quantity of DU (R1 and R2).

There are eight types of Uranium mines, ports, UOC Agents permits depending on activity.

U1	Mine
U2	Land (Rail/Road)
U3	Sea
U4	Storage
U5	Broker
U6	Laboratory
U7	Establish Mine (EF)
U8	Decommission Mine

The process to develop templates for permits U1, U7 and U8 has begun but yet to be completed.

UOC Permit conditions relating to accountancy are:

- Enable timely and accurate preparation of accountancy reports - recording all UOC inventory and changes,
- inventory changes recorded on day change occurs or is calculated,
- determine the precision and accuracy of measurements and estimate measurement uncertainties,

- provide for the timely investigation and resolution of any accounting anomaly indicating a possible loss of UOC,
- Locate any particular item on inventory in <2 hrs,
- Make measurements to support accountancy,
- Record movement of samples,
- Conduct inventory stock-take every 6 months - reported to ASNO,
- Minimise shipper/receiver differences.

Each export of UOC is subject to case-by-case approval:

- Verified through export controls and customs authorities,
- Shipper weights checked against received weights through nuclear cooperation agreements,
- Seek to minimise shipper/receiver differences.

Every six months, mines provide a summary report of production, stocks and exports.

Mines typically conduct monthly production reconciliation, which is not reported to ASNO. There is no requirement to report to ASNO on in-process inventories.

XIII.2 Special Permit Issued to ANSTO

Key NMAC provisions in the ANSTO permit that assist nuclear security are:

- accept and apply all containment and surveillance measures which the Director General may require from time to time;
- identify diversion or unauthorised access scenarios for nuclear material and associated items by insiders, taking into account the sensitivity of the material and establish measures to prevent or detect such diversion;
- assess the expected losses from any anticipated handling or processing of nuclear material;
- identify, review and evaluate shipper/receiver differences;
- evaluate accumulations of unmeasured inventory and unmeasured losses;
- include procedures for investigating and correcting any discrepancies discovered between the inventory; and
- accountancy and control arrangements done for the purposes of IAEA safeguards.

Handling and possessing of nuclear material without a permit is prohibited according to the Safeguards Act, Part II, Division 1. The Safeguards Act establishes penalties for violations of permit requirements. Penalties are established also for obstruction of IAEA inspectors and unauthorized access to areas to which access is restricted under a permit.

Permits issued under Safeguards Act contain both NMAC and physical security requirements. Inspections of uranium mines and small quantity permit holders typically cover both NMAC and security requirements while inspections at ANSTO cover each topic individually. In any case ASNO

takes into account synergies between NMAC and security in setting requirements and conducting inspections.

XIII.3 ASNO Database

ASNO has established NUMBAT - Nuclear Material Balances and Tracking database which includes:

- Register of permit holders,
- Nuclear material inventories of individual permit holders,
- Fulfil reporting requirements to IAEA (ICRs, PILs, MBRs),
- Register of national and IAEA and inspections and inspectors,
- Tracking of Australian obligated nuclear material pursuant to Australia's network of nuclear cooperation agreements.

The IPPAS team was informed that reports from the facilities to ASNO are transferred via open e-mail (excel and pdf files are attached), noting that these reports do not contain details on the locations of nuclear material and that emails between Australian government entities offer a level of protection. ASNO uploads the records to the IAEA reporting system directly.

The database is currently undergoing redevelopment to include external functionality for permit holders. The new database will allow permit holders to log-in to submit reports and manage their nuclear material inventories.

According to information received, the IPPAS team assessed that:

- State System for Accountancy and Control (SSAC system) supports the nuclear security regime,
- Measures are taken to ensure effective accounting and control of nuclear material in the State, and
- Handling and possessing of nuclear material without an appropriate permit is prohibited.

The IPPAS team was informed that:

- Unauthorized removal of nuclear material and insider threat is considered as a credible risk in state's nuclear security threat assessment and the DBT;
- Graded approach is applied for nuclear security requirements, including accounting and control. Australia uses system of categorization of nuclear material in line with NSS-13;
- Australia periodically reviews experience in nuclear security (including NMAC) and addresses issues/problems identified;
- Requirements for reporting and investigating nuclear security events concerning nuclear material are established;
- Rules and procedures for reporting losses are established;
- Opportunities are provided for personnel (from facility and State authorities) to be trained in nuclear security issues including NMAC (all inspectors have received basic IAEA SSAC training course);

- Requirements for security of information systems used for accounting and control are applied.

XIII.4 Regulatory Oversight of NMAC System Implementation

The State system for accountancy and control is established primarily to meet IAEA safeguards requirements however this system also supports the nuclear security regime. Competent authority (ASNO) has been established for this purpose. IPPAS team was informed that the Section for IAEA Safeguards (with four properly trained employees) is part of the ASNO organizational structure. NMAC is a part of licencing requirements taking account of the graded approach. Violations of NMAC requirements are subject to sanctions. The IPPAS team was also informed that ASNO may conduct NMAC inspections before IAEA PIVs or concurrent with operator PITs. However, PITs and PIVs conducted for IAEA safeguards purposes may not be sufficient to ensure the timely detection of unauthorised removal of nuclear material.

Suggestion 14 (2017): ASNO should consider requiring additional NMAC activities in permits and conducting related NMAC inspections, on a graded approach, to ensure timely detection of discrepancies and unauthorised removal of nuclear material.

Australia has appropriate operational experience and expertise in nuclear security including NMAC issues.

The IPPAS team was informed that:

- The NMAC system is periodically inspected and evaluated through self-assessment and inspection activities by IAEA Safeguards personnel,
- Australia established points of contact in case of nuclear material is lost or found,
- Australia promotes nuclear security culture and NMAC is included in such promotion.

XIV. FACILITY LEVEL REVIEW

ANSTO has issued a Security and Safeguards Policy. The policy sets out the overall framework for the arrangements by which ANSTO manages the security of its radioactive material and the security and safeguarding of its nuclear material.

ANSTO has a Permit to possess nuclear materials and associated items. Compliance Codes attached to this permit include:

- Plans, procedures and arrangements,
- Management authority and responsibilities,
- Control of nuclear material and associated items,
- Safeguards & Security Objectives / Requirements ,
- Records & Reporting.

ANSTO established a Security and Safeguards Oversight Committee (SSOC) - responsible to CEO and its membership includes

- Manager Nuclear Security,
- Manager Nuclear Safeguards,
- Leader Nuclear Stewardship,
- Manager Regulatory Affairs,
- Manager International Affairs,
- Group Executive PCSS,
- Others by invitation.

The SSOC provides direct assurance and oversight of issues and risks in security and safeguards matters relating to the organisation. The SSOC is a forum to identify process improvements, systemic issues and encompasses a holistic approach to sharing information with the CEO of ANSTO of organisational significance. The committee operates under a "no blame full disclosure" mandate and all members are empowered to accurately and factually report matters of concern, for decision by the CEO and the General Manager PCSS.

XIV.1 Managing the NMAC System

ANSTO has established a Nuclear Safeguards Office with two employees (Nuclear Safeguards Manager and Nuclear Safeguards Officer). In each facility within ANSTO site there are designated individuals responsible for compliance (Safeguards Authorised Officers - 12 persons).

Documents issued by the ANSTO Nuclear Safeguards Office are:

- NMAC plan,
- Safeguards manual, and
- Procedures and instructions.

Each facility that has material subject to NMAC controls is required to establish and maintain effective operational records and operational procedures for safeguards controls.

MBAs and associated KMPs in ANSTO are described in the following table:

MBA	Name	No of KMP	Details and Status
AS-C	Research and Development Labs	3	^{99}Mo production using LEU targets & storage
AS-D	Vault Storage	3	Storage of seldom used material
AS-F	OPAL Reactor	4	Open Pool Australian Light-Water (LEU)

The IPPAS team was informed that safeguards and security offices communicate on a daily basis and they are obliged to prepare and submit monthly report to the SSOC.

XIV.2 Records

All nuclear materials in ANSTO are received in form of a batch (single item). A record about each single item consists of a unique ID, and data about isotope content and weight.

The IPPAS team observed that NMAC records are managed in a centralised database which is operated by ANSTO's Nuclear Safeguards Office. Records are prepared and maintained that document all nuclear materials from receipt in ANSTO to transfer out from the facility. Records are prepared to document every activity as it occurs. The Nuclear Safeguards Office receives records in paper (signed) and in electronic format. Records are then uploaded to the database which enables the system to track each item with an assigned process. The program is capable of generating up-to-date book inventory lists on request. Backup copies are generated of all records and reports on a daily basis and these records are stored in a separate secure location. Accuracy of records is assured by effective supervision.

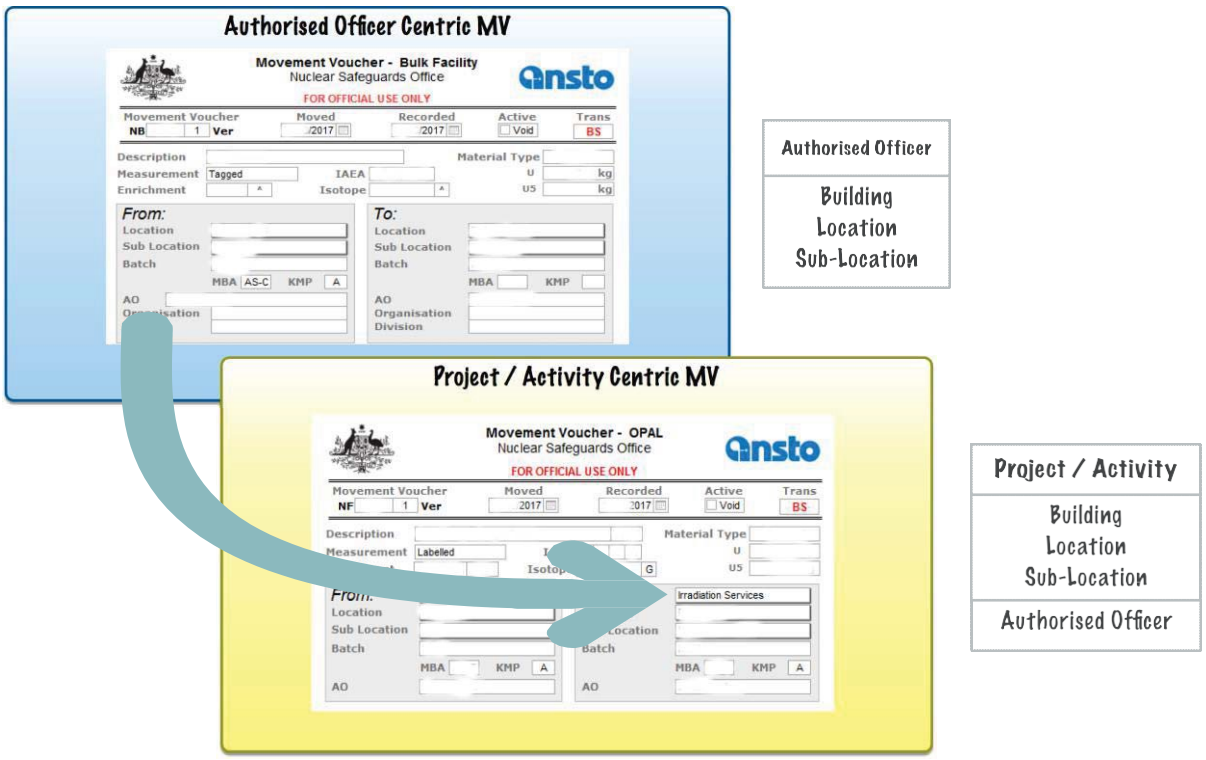

Figure 3: NMAC forms used at ANSTO

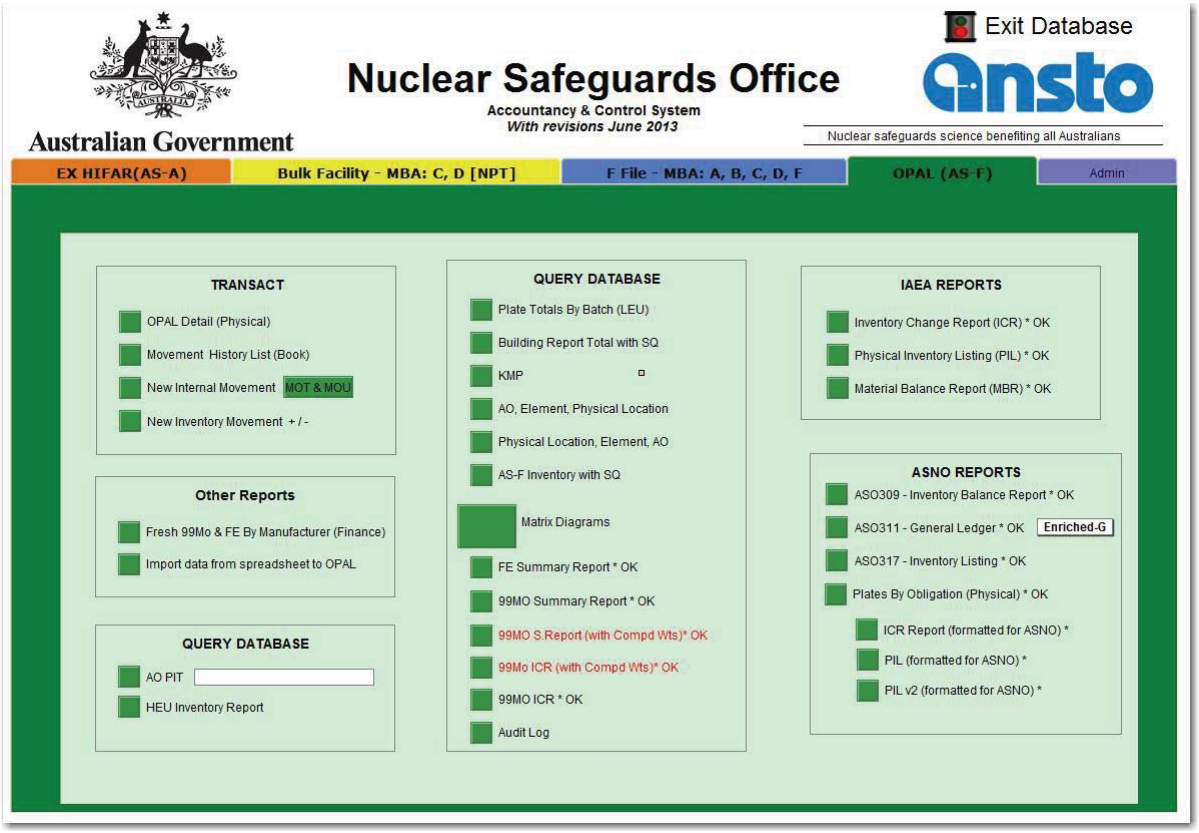

Figure 4: NMAC database at ANSTO

XIV.3 Physical Inventory Taking of Nuclear Materials

The IPPAS team was informed that specific inventory instructions are prepared for every physical inventory taking. The results of the physical inventory taking are reflected in the prepared inventory lists and in the material accounting records.

Every facility within ANSTO has the means in place to conduct a physical inventory to confirm the location of nuclear material and the accuracy of the book inventory.

XIV.4 Measurement and Measurement Quality Control

KMPs are established in accordance with the ASNO permit and IAEA requirements. The IPPAS team was informed that measurements can be done in certified laboratories on request.

XIV.5 Nuclear Material Control

The IPPAS team was informed that all personnel and activities are subject to the process of authorisation. A process for granting/revoking access for personnel to computers where data concerning nuclear material is stored and processed exists. Safeguards Authorised Officers are obliged to maintain accurate records and regularly control the inventory of nuclear material (or associated items). The IPPAS team observed that there are numerous types and places for material containment, e.g. cans, glove boxes, storage cabinets, rooms and vaults.

The IPPAS team observed and/or was informed that measures have been applied for detection of unauthorized introduction, transfer or removal of nuclear material such as:

XIV.6 Nuclear Material Movements

The IPPAS team was informed that appropriate procedures for shipments are established and that an Officer is present during each shipment. Movements of nuclear material are clearly documented, and records are updated accordingly. Movement of nuclear material requires authorisation. Shipper-receiver differences are investigated immediately.

XIV.7 Detection, Investigation and Resolution of Irregularities

The IPPAS team was informed that ANSTO has implemented ISO 9001 Certification and that programmes for reporting, investing, documenting and resolving irregularities (including corrective actions) are in place. ANSTO uses the Safeguard Report System for detection, investigation and resolution of irregularities.

XIV.8 Assessment and Performance Testing of the NMAC System

The IPPAS team was informed that the ANSTO Safeguards Office continuously improves the NMAC system. A Business Management System Documents Plan has been developed and implemented. Improvement plans include:

- Implement improved checklist for PIT arrangements by Q1 2018,
- Revised Audit Program to be formalized during CY 2018,
- Development of LMS training modules following Business Management System documents Q3/Q4 2018,
- Development of a Training Curriculum,
    - Introduction to safeguards,
    - Permits and compliance,

- Accountancy and control,
- Notification and reporting,
- Inspections.

The IPPAS team was informed that revision of all documents including the Safeguards Manual will be completed by the end of Q2 2018.

RESPONSE TO RECOMMENDATIONS AND SUGGESTIONS PROVIDED DURING THE 2013 IPPAS MISSION

This chapter aims at summarizing the recommendations and suggestions provided during the IPPAS Mission conducted in 2013, the responses provided by ASNO, ARPANSA and ANSTO in the Advanced Information Package and in the presentations delivered by Australian experts and their updates provided during and after the discussion with the IPPAS team, as well as the evaluation of the progress made by the IPPAS team.

XV. STATE LEVEL RECOMMENDATIONS AND SUGGESTIONS

XV.1 Government Organization, Assignment of Responsibilities and International Obligations

Recommendation 1: The Australian Government should introduce a requirement for a regular review and update of the physical protection regime

Response: This recommendation is being met through the following actions:

- All Australian regulators are subject to:
    - Regulator Performance Framework - Australian Government Regulatory Principles (No. 9 - "All regulation must be periodically reviewed to test its continuing relevance")
    - Commonwealth Risk Management Policy (Element No. 9 - "Reviewing and continuously improving the management of risk.")
- Australia's nuclear governance arrangements were reviewed as part of the Federal Government's response to the South Australian Nuclear Fuel Cycle Royal Commission report. The Australian Government made no recommendations for change.
- ASNO's regulatory requirements are reviewed during the process to extend permits to possess nuclear material (usually every 5-10 years).
    - ASNO recently started a series of rolling reviews of all regulatory requirements and reformatting of all permits.
- ASNO conducts regular reviews of the Design Basis Threat.
- ASNO is developing a Quality Management System which will underpin the operation of ASNO's regulatory activities, including the provision for regular review.

It is not seen as necessary to formalise these policies and activities in the specific enacting legislation (i.e. the *Nuclear Non-Proliferation (Safeguards) Act l987*).

Team evaluation: The IPPAS team noted the response to this recommendation and was further advised that the regime also performs reviews and opportunities for improvements based on lessons learned arising from participation in national and international exercises such as the GICNT KANGAROO HARBOUR Exercise and other experiences gained through operational experience, activities at the regional level and outcomes from the Nuclear Agencies Consulting Committee. The IPPAS team assessed that this recommendation has been addressed.

XV.2 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.

Response: ASNO and ARPANSA contend that the Safeguards Act and ARPANS Act provide for sufficient sanctions. Firstly, the "Crown immunity" set out in Section 7(2) of the Safeguards Act and Section 4(2) of the ARPANS Act does not apply to corporate Commonwealth entities (CCEs) including ANSTO and CSIRO and only to non-corporate Commonwealth entities (NCCEs) such as ASNO, ARPANSA and the Department of Defence. Secondly, "Crown immunity" does not apply to individuals acting outside of the scope of their instruction from the entity (permit or license holder). Finally, notwithstanding that where "Crown immunity" provides an exemption from prosecution, there are other actions that can be taken that amount to sanction and/or enforcement (e.g. withdrawal of permit/license, orders & directions, improvement notices, warrants and reporting to parliament).

Team evaluation: The IPPAS Team agreed with the assessment made by the Government of Australia. In essence, while Crown Immunity applies to the government entity, it does not apply to a government official that is violating rules or laws. On the basis of the response and discussions during the course of the IPPAS mission, the IPPAS team assessed that this recommendation has been adequately addressed.

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".

Response: CEO ARPANSA has the power to direct controlled persons under Section 41 of the ARPANS Act to, inter alia, to accept prime responsibility for orphaned material, especially in order to protect the health and safety of people or to avoid damage to the environment. The licence holder's authority and capability to hold such material will have to be taken into account. The use of this power will also take into account ASNO's regulatory powers and responsibilities (which has

similar power to issue Directions) and will be dealt with on a case-by-case basis given the infrequency and diversity of such cases.

Note, however that CEO ARPANSA's power to direct under Section 41 is restricted to controlled persons, who are defined in Section 13 of the ARPANS Act.

Team evaluation: The IPPAS team assessed that based the response provided and discussions during the IPPAS mission that this issue has been satisfactorily addressed and that adequate provisions exist for regaining control and responsibility for material found to be out of regulatory control.

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.

Response: ARPANSA has developed Radiation Protection Series No.11 Code of Practice on the Security of Radioactive Material (2006). This Code is captured formally under the National Director of Radiation Protection (NDRP), which directly links to all jurisdictions, as required under the COAG agreement. The purpose of the NDRP is to provide an agreed framework for radiation safety, including both ionizing and non-ionizing radiation, together with clear regulatory statements to be adopted by the Commonwealth, States and Territories. The Australian Health Ministers' Conference (AHMC) agreed that upon consideration and approval of the provisions of the Directory, the regulatory elements of the Directory shall be adopted in each jurisdiction as soon as possible, using existing Commonwealth/State/Territory regulatory frameworks.

All jurisdictions have adopted the RPS-11 requirements in one form or another. In order to assist the implementation of these requirements, ARPANSA has conducted the following:

- Developed a pool of nationally accredited assessors who are trained to develop, review and endorse source security plans in accordance the requirements of the Code (approved only by the regulatory body).
- Developed a suite of Practice Specific Security Guides (PSSGs) to assist in the practical implementation of the requirements of the Code.

ARPANSA believes it has fulfilled the suggestion**.**

Note however that the publication of RPS 11 and the promotion of its adoption and use in the States and Territories was also the situation in 2013. It is noted from the lead-in text of the 2013 IPPAS report that Suggestion 2 was made on the expectation that something more could be done formally to "ensure" uniformity. However, under current Constitutional arrangements, the CEO of ARPANSA can only promote uniformity as his jurisdiction is only over Commonwealth entities and Commonwealth contractors and their employees.

Team evaluation: Based on the response provided and discussions during the IPPAS Mission that adequate measures exist to ensure uniformity of requirements.

The IPPAS team was not provided assurance that such harmonization of requirements would or could be performed in a timely manner. It is recognized that the Commonwealth lacks authority in this matter. The IPPAS team assessed that this suggestion has been addressed.

Recommendation 3: The Australian Government should promulgate nuclear security requirements in regulations.

Response: Physical Protection requirements are currently set in permits issued under the Safeguards Act. Criminal penalties apply to contravening a condition of permit (see Section 25 of the Act). As such, permit conditions fulfil the role of effecting physical protection requirements otherwise set in regulations. It is not viable to promulgate nuclear security requirements in regulations given the current scope of Australia's nuclear activities and under current government policy with regard to regulatory reform (see https://www.pmc.gov.au/regulation/australias-approach-regulatory-reform).

Team evaluation: This recommendation was based on the fact that *NSS 20, paragraph 3.3 (e) states that the legislative and regulatory framework, to govern the nuclear security regime* provide for the establishment of nuclear security regulations and requirements. In addition, *NSS l3, paragraph 3.ll states that the State's legislation should provide for a 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.

One of the primary reasons to establish regulations/requirements is to make sure that all stakeholders can understand what is expected with regards to the security of the nuclear material and nuclear facilities. A regulation is a type of requirement that is very structured and may involve significant resources and time to promulgate. ASNO has opted to take an alternate approach. Since the last IPPAS Mission, ASNO has developed generic permitting documents that can be used for the different types of facilities they regulate. Within these permitting documents, they specify the security requirements for the facilities. These generic permitting documents will be published on-line so that all stakeholders will have access to them. Given the limited number of facilities that may be subject to the requirements, as well as the current practice of States to reduce the numbers of regulations, this appears to be an effective way to meet the intent of the recommendations, allowing timely issuance without adverse impact on budgets.

On the basis of the response and discussions during the course of the IPPAS mission, the IPPAS team assessed that this recommendation has been adequately addressed.

XV.3 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.

Response: As part of a review of all staffing of the Department of Foreign Affairs and Trade in 2015, ASNO's overall staffing (including for nuclear security) was reviewed. The outcome of the review was the allocation of an extra position to cover, inter alia, quality management. This position supports all of ASNO's regulatory activities, including nuclear security. Another Departmental staffing review is currently in progress.

Team evaluation: The IPPAS team has considered the response to this suggestion. This IPPAS follow-up mission has made a similar suggestion in Chapter VI.1 of this report.

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.

Response: In June 2016 ARPANSA issued informal advice which set the URC as 50 mSv and linked the level of HRC to radiological consequences (irrespective of whether caused by accident or sabotage) that require urgent protective actions under ARPANSA's Draft Emergency Exposure Guide (based on IAEA GSR Part 7). Once these have been formally communicated, ASNO plans to adopt these levels, upon which the recommendation and suggestion will have been met.

ARPANSA has developed the definitions as well as a procedure for developing the level for HRC. Next step is to promulgate the definitions as regulatory requirements and guidelines for ARPANSA licence holders. Following discussion with State/Territory regulators, the definitions may be included in the National Directory for Radiation Protection (NDRP) and/or the ARPANSA Emergency Exposure Guide (to be published).

Team evaluation: Based on the response provided and additional information and discussion during this IPPAS Mission, the IPPAS team assessed that the URC and HRC have been established. However, the IPPAS team was not informed of the methodology that a permit holder would use to apply the URC and HRC when performing assessment of their facilities and determining minimum adequate security measures based on analysis outcomes. For the assessment the permit holder needs to be advised about factors such as exposure time, type and location of reference human as well as exposure pathways. The IPPAS team encourage ARPANSA to issue the detailed guidance which sets the URC as 50 mSv and the Emergency Exposure Guide in a timely manner.

IPPAS team assessed that this recommendation and suggestion have been adequately addressed.

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.

Response: Current arrangements for detections of radioactive material at the border include an immediate notification to ARPANSA, and also to ASNO for nuclear material. Typically, ARPANSA joins with the Australian Border Force in order to investigate the matter. This may include interactions with the jurisdictional regulator to ensure that regulatory control of the material is maintained. If additional search and seizure capacity is required, jurisdictions have two (2) specific national plans that they can call upon:

(1) Commonwealth Disaster Plan (COMDISPLAN) - where ARPANSA field deployable teams can be activated to assist a jurisdictional authority

(2) National Counter Terrorism Plan (NCTP) - where ARPANSA's specialist field teams can be called upon to assist any authority

Furthermore, within the region Australian RANET-registered capabilities can also assist internationally.

ARPANSA was funded in early 2000, specifically to develop a capability that could be deployed at any time in order to locate and recover materials out of regulatory control. These arrangements and capabilities have been tested with a number of real-world events in Australia at the border. Most recently, intercepted contaminated material was notified to ARPANSA in early 2017, where subsequent analysis and investigation was conducted and the materials placed under regulatory control. (See ITDB Report 2017-06-006 (AUL-17-001))

ARPANSA intends to continue to pursue a more comprehensive Nuclear and Radiological Border Detection Strategy (consistent with NSS-26) for the implementation of more advanced technology and a more comprehensive CONOPS. This will take many years to develop given the recent and future changes for government policy development agencies. ARPANSA believes that Australia has the capability, capacity and arrangements that have demonstrated the expectation of this recommendation.

The "Arrangements" referred are in place. They were tested during Exercise Pacific Protector among ARPANSA, ANSTO, ASNO and the ABF in September 2017.

Team evaluation: Based on the response provided, the IPPAS team assessed that this recommendation has been addressed.

XV.4 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.

Response: NSS-14 is not a licence condition. Instead, it is acknowledged as international best practice in our regulatory requirements, which has been promulgated through the Regulatory Guide: Plans and Arrangements for Managing Safety (REG-LA-SUP-280B, September 2017) at pp 25 to 27.

Team evaluation: Based on the response provided and discussion with ARPANSA, the IPPAS team assessed that this recommendation has been addressed.

Suggestion 5: The Australian Government should consider developing clear requirements for material that is both radioactive and nuclear at the same time.

Response: ASNO and ARPANSA use the principles set out in NSS No. 13 (paras 4.2 & 6.1) and NSS No. 14 (paras 1.15 & 1.16). Permit PN001 (ANSTO) sets out guidance regarding the security of nuclear material that is also radiologically hazardous. Outside of ANSTO, the number of instances where dual requirements apply are small, which are treated case-by-case, and does not warrant a dedicated guidance document. ASNO and ARPANSA believe this suggestion is satisfactorily met.

Team evaluation: Based on the response provided and permit reviews, the IPPAS team assessed that this suggestion has been addressed.

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.

Response: ARPANSA intends to update RPS-11 when the IAEA NSS-11 comes into effect. This will capture re-ordering for consistency with the international community, noting that it does not adversely impact the performance expectation of the protective security system.

Team evaluation: Based on the response provided, the IPPAS Team assessed that ARPANSA committed to amend the RPS-11 according to the suggestion. This suggestion is still outstanding.

Suggestion 7: ARPANSA should consider taking appropriate steps to retain the regulatory role delegated to it by the ARPANS Act.

Response: ARPANSA has retained the regulatory role delegated to it under the ARPANSA Act. ARPANSA-trained protective security advisors assist State and Territory jurisdictions in assessing and advising on security plans, the regulators retain their roles also, which is to approve plans. ARPANSA believes it already meets the suggestion.

The lead in text in page 20 of the IPPAS 2013 report provides the context for this suggestion. It states: "In the case of Category 1-3 radioactive sources the user …. 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."

The observation that "accredited private entities can assess and endorse security plans on behalf of the state or territory regulator" is not correct. A security plan that is endorsed by an accredited assessor is not done on behalf of the regulator. The endorsed security plan will require the approval of the regulator. Therefore ARPANSA (and the State/Territory regulators) never delegated their respective regulatory roles.

Team evaluation: Based on the response provided and discussion with ARPANSA regarding their operational experience with the process since it was implemented, the IPPAS team assessed that this suggestion has been addressed.

Suggestion 8: The maximum licensed activity should provide basis for both safety and security arrangements.

Response: The lead in text in page 21 of the 2013 IPPAS report shows that the concern that led to the suggestion was on the basis of a Source Security Plan of ANSTO prepared on 16 October 2013. ARPANSA can confirm that its regulatory requirements are that the licence holder must ensure that its security arrangements for facilities and sources are in accordance with the physical security requirements in Chapter 3 of RPS 11, which is a statutory licence condition. This requirement is also in the Regulatory Guide: Plans and Arrangements for Managing Safety (REG-LA-SUP-280B, September 2017). Once a licence holder includes an arrangement in its Plans and Arrangements, the licence holder must take steps to implement it or face the prospect of being found in breach of Regulation 49.

Team evaluation: Based on the response and discussions during the mission, the IPPAS team noted that ARPANSA is actively working to resolve this suggestion.

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.

Response: In 2016, through the Radiation Health Committee (all regulators), members agreed to abandon the National Sealed Source Register (NSSR) and replace this with a Network of National Registers which can be called upon by contacting the relevant jurisdictional radiation regulator at any time. This approach acknowledged that the complexity of operating a system which accesses nine (9) different database systems was technically and commercially challenging, and heeded the Australian Government policy which expects an 'enter once, use multiple times' approach to managing data. Some regulators were manually

extracting and entering data into the NSSR, as automation was not feasible due to resources. ARPANSA retains a record of all imports and all high activity exports entering and exiting the country. ARPANSA retains all sources held by Commonwealth licence holders through our Licence Administration Database (LAD). ARPANSA can call upon any jurisdiction to gain source data at any time, and has done so during investigations in recent times. The results have included actual prosecutions. ARPANSA believes this system is working well.

Changes in circumstances led to a single national register becoming too costly and difficult to continue to implement within a Federal-State system in which there are nine radiation regulators. However, source registers exist in each jurisdiction and the information can be shared easily through other means of communications.

Team evaluation: The IPPAS team assessed that based on the response and discussions that the expectations of the Code of Conduct Paragraph 11 are not being met and will change this suggestion to a new recommendation. (See new Recommendation 1 in the 2017 IPPAS Mission Report).

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.

Response: ARPANSA agrees. Security advisors, or experts, within ARPANSA have been elevated to inspector status with a structural change in the regulatory branch. Safety, Security and EPR have now all been integrated into the compliance and enforcement regime. ARPANSA Performance Objectives and Criteria (PO&C's) now form the basis of all inspections for both controlled material, controlled apparatus and facilities.

The lead in text in page 22 of the IPPAS 2013 report was correct at the time of the publication where it stated that security advisers were not inspectors. However, the situation has since changed and the suggestion has been implemented. Inspectors are now trained to have both safety and security expertise. See also the presentation by Mr Jim Scott for more details on how safety-security synergy is integrated into the Performance Objectives and Criteria and how this translates into inspector training.

Team evaluation: Based on the response provided and discussion with ARPANSA, the IPPAS team assessed that this suggestion has been addressed.

XV.5 Integration & Participation of Other Organizations

Suggestion 11: The Australian Government should consider producing a classification guide that is more specific and relevant to nuclear and radiological issues.

Response: ASNO has developed a draft classification guide for nuclear material and associated technology. The concept for the guide will be explained during the mission.

Team evaluation: The IPPAS team was provided the draft guide for review. Once the guide is complete and implemented, there will be higher confidence that information and information systems will receive the appropriate level of protection.

The IPPAS team notes that this suggestion remains under development and encourages both regulatory bodies to work together to develop a single uniform classification guide. The suggestion will continue to be open until the guide is put in final form and put into use.

Recommendation 7: The Australian Government should ensure a uniform approach to information security for all regulated licensees/permit holders.

Response: This matter is outside of the scope of the previous and current IPPAS mission. Information security is uniform where the Australian Government Protective Security Policy Framework (PSPF) applies. ASNO and ARPANSA both use the PSPF for their respective regulated licensees/permit holders. It is not possible to impose PSPF requirements on Australian States and Territories.

Almost all of ARPANSA's licence holders are Commonwealth entities, who must comply with the requirements of the PSPF, which is an Australian Government requirement.

From the lead-in text in page 24 of the IPPAS 2013 report, it is noted that Recommendation 7 was made because there are different standards of information security between the Commonwealth and State regulated entities. As acknowledged in page 23 of the IPPAS 2013 report, this was out of the scope of the IPPAS mission.

Team evaluation: It is recognized that the Commonwealth lacks authority in this matter. The IPPAS team assessed that this suggestion has been addressed.

XV.6 Threat Assessment & Design Basis Threat

Suggestion 12: The Australian Government should consider a more regular review of the DBT to take into account the changing environment.

Suggestion 13: The Australian Government should consider including ———————— attack threats as part of its DBT.

Response: Australia conducted a mid-term review of the DBT in 2017, which resulted in a revision being issued in June 2017. This review considered ———— threats, including from unmanned aerial vehicles (drones). ASNO has developed a procedure for the regular interim (minor) review of the DBT.

Team evaluation: Based on the response provided and discussion with ASNO, the IPPAS team assessed that these suggestions have been addressed.

XV.7 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.

Response: Balanced protection is considered during the design and construction of new buildings. In accordance with the ANSTO Security Plan 2017, classified adversary sequence diagrams are used to assess balanced protection and the ANSTO Security Exercise Program is used to test any potential vulnerabilities. The Security Plan provides guidance on the application of balanced protection in the design of ANSTO's physical protection system and outlines the process of regular security system evaluation.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

XVI. FACILITY LEVEL RECOMMENDATIONS AND SUGGESTIONS

XVI.1 Facility Implementation of Physical Protection System at ANSTO

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.

Response: The latest version of the ANSTO Security Plan was completed in 2017. This Plan is part of ANSTO's Security Strategy documents and supports ANSTO's Protective Security Strategy 2016-2018 as it was deemed not feasible to integrate all plans into one for various reasons. The Plan is designed to provide overarching guidance across different security related plans, including individual facility plans. Section 20 of the Plan provides guidance on the design, evaluation and maintenance of the physical security system as determined by business impact levels (i.e. consequences).

Team evaluation: The latest version of the ANSTO Security Plan was completed in 2017 and is to be seen as a useful strategy document. The team acknowledges that it provides overarching guidance across different security related plans. The IPPAS team assessed that this suggestion has been addressed.

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.

Response: ANSTO engaged Nippon Telegraph and Telephone (NTT) Security to perform an external vulnerability assessment during 2017. This test was completed successfully and provided assurance that the likelihood of an external attacker accessing ANSTO systems is highly unlikely. ———————————

Team evaluation: The IPPAS team was not able to review the NTT assessment report, but was able to interview the Information Technology Security Advisor and Technical Information Technology Security Officer on the NSS 17 Computer Security controls and implementations. The review was focused on the network architectures, monitoring and detection, access controls, media protections, change control, physical security, and protective measures for critical information and systems. This review was completed to identify if appropriate controls are in place to protect the critical networks and environments. The IPPAS team was also able to visit the data diode location to validate that the device for OPALNet was isolated and secure. Based on the review, this suggestion has been addressed.

Suggestion 17: ANSTO should consider formally re-evaluating the classification of both ——————— 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.

Response: ——— has been re-evaluated in accordance with ANSTO's Security Manual, which derives its classification requirements from the PSPF Information Security Management Guidelines, Australian Government Security Classification System. ——— has not yet been reclassified due to organisational priorities.

Team evaluation: The re-evaluation of —— did not include the NSS 17 Computer Security for Nuclear Facilities, however the IPPAS team completed a comparison of the PSPF and ISM against the NSS 17 controls. Based on the comparison, and the re-assessment that was completed on ——, The IPPAS team accepts the reclassification for ——.

However, there has not been a re-evaluation of the ——, so this Suggestion remains open until the ——— is re-evaluated. ASNO will produce a Classification Guide that will assist in the re-evaluation to help identify the security zone for ————and the required controls to protect the environment.

Suggestion 18: ANSTO should consider improving control of access to the ———— office to employ two-factor authentication (i.e. proximity and PIN) at all times.

Response: Two-factor authentication for access to the ———— office was established and has been employed since August 2014.

Team evaluation: Based on the response provided, field observations and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

XVI.2 On-site and Off-site Response

Suggestion 19: ANSTO should consider establishing a process for the independent verification of guard force performance.

Response: The current Memorandum of Understanding (MoU) between ANSTO and AFP (2015-2019) sets the terms and conditions (including service standards) to be met by the on-site Australian Federal Police (AFP) in connection with the delivery of 'protective services' at ANSTO. This MoU is subject to an approved annual Internal Audit Program which assesses and rates the agreed Performance Measures / Key Performance Indicators (KPIs) listed in Schedule A of the MoU. In accordance with Schedule A, these KPIs (listed in Section 5 of the ANSTO Security Plan) are reported and reviewed on a monthly basis. Independent verification of guard force performance is established through force-on-force exercises which range from internal to multi-agency exercises.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

Suggestion 20: ANSTO should consider the appropriateness of current staffing levels of the SCC.

Response: In 2014, ANSTO reviewed the staffing arrangements for the SCC (now ANSTO Security Operations Centre - ASOC), and upon regulatory approval, increased staffing to — specialist Control Room Operators (— security contractors). This change allowed the Australian Federal Police (AFP) to focus on core duties.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

XVI.3 Out of Fence & from Perimeter Fence to Buildings

Suggestion 21: ANSTO should consider prioritising the programming of detection analytics for building —.

Response: The perimeter CCTV security system has been upgraded to a ———— detection capability for the entire perimeter of ANSTO Lucas Heights following this

IPPAS suggestion. This enables first point of detection to occur external to site and is used in conjunction with 24 hour active monitoring by the ASOC and AFP, physical delay and response measures. The building — operating license has been approved and issued on the basis of the existing security system design since the facility's inception, prior to the IPPAS mission in 2013. Recent physical security upgrades have been undertaken and approved by the regulator due to an increase in operating requirements. ANSTO deems the existing security system arrangements to be adequate following the perimeter security system upgrades, and defence-in-depth security measures outlined above.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

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

Response: _____

Team evaluation: _____

XVI.4 Building —

Suggestion 23: Building — would benefit from external CCTV in order to verify any alarms triggered by unauthorized access.

Response: The perimeter security system has been upgraded to a ———— detection system for the entire perimeter of ANSTO Lucas Heights since this suggestion. This enables first point detection of path elements and potential adversary routes to occur external to the site.

ANSTO is also pursuing continuous improvement opportunities (risk-based, intelligence-led approach), by engaging the facility licence holder to review and update security plans and arrangements, including internal immediate detection capabilities.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

XVI.5 Building —

Recommendation 8: ANSTO should apply detection measures on potential adversary routes into the ——————— production facility by-passing the routes currently covered by detection measures.

Response: The perimeter CCTV security system has been upgraded to a ——— detection capability for the entire perimeter of ANSTO Lucas Heights. This enables first point detection of path elements and potential adversary routes to occur external to the site, mitigating the need for detection measures specific to the ——— building. Additional ——————————— cameras have been installed to provide an enhanced assessment capability for ANSTO. These cameras provide an assessment capability in the ——— building area.

Regarding the ——— facility, ANSTO has also positioned a dedicated perimeter camera to cover ——— entry points to further strengthen detection measures, and engaged the facility licence holder to install a ——————— for immediate detection at point of entry.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this recommendation has been addressed.

XVI.6 Building —

Recommendation 9: ANSTO should apply detection measures on potential adversary routes into the ——— facility by-passing the routes currently covered by detection measures.

Response: The perimeter CCTV security system has been upgraded to a ——— detection capability for the entire perimeter of ANSTO Lucas Heights. This enables first point detection of path elements and potential adversary routes to occur external to the site, mitigating the need for detection measures specific to the ——— building. Additional ——————————— cameras have been installed to provide an enhanced assessment capability for ANSTO. These cameras provide an assessment capability in the ——— building area.

Regarding the ——— facility, ANSTO has also positioned a dedicated perimeter camera to cover ——— entry points to further strengthen detection measures, and engaged the facility licence holder to install a ——————— for immediate detection at point of entry.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this recommendation has been addressed.

XVI.7 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.

Response: Relevant Security Plans have been updated. ARPANSA deem placarding unnecessary if the transport is under armed escort. All stipulations are addressed by ANSTO incorporating an armed escort (AFP) into every ANSTO Transport Security Plan.

Team evaluation: Based on the response provided and discussion with ANSTO the IPPAS team assessed that this suggestion has been addressed.

According to the international good practice, the countries hosting an IPPAS mission establish an action plan, subsequent to the IPPAS mission, to implement the recommendations and suggestions provided in the IPPAS report. The action plan includes the responsible organisations, the tasks to be completed and the deadline for completion. The progress of the tasks is also monitored.

Suggestion 15 (2017): ASNO, ARPANSA and ANSTO should consider implementing the recommendations and suggestions provided in the IPPAS report in a timely and systematic manner.

The IPPAS team noted that considerable efforts have been undertaken by ASNO, ARPANSA and ANSTO to address Recommendations and Suggestions arising from the 2013 IPPAS Mission report. The IPPAS team assesses that these efforts will serve to strengthen Australia's nuclear security regime.

It is noted however that some efforts to address Recommendations and Suggestions remain a work in progress. The IPPAS team encourages expedited and continued efforts to address these issues in a timely fashion to the extent possible while recognizing the challenges of achieving resolutions are sometimes cumbersome and complicated.

ACKNOWLEDGEMENTS

During the IPPAS mission the IPPAS team experienced outstanding cooperation from personnel at all technical and administrative levels. Indeed, the practical arrangements made by ASNO, ARPANSA and ANSTO for the facilitation of the mission were excellent and could serve as example to other countries planning to host such an engagement. The IPPAS mission team noted that all those who participated in the meetings and discussions were interested in obtaining international experience and advice on ways to conduct their work and perform their duties. Additionally, notwithstanding the need to exercise discretion with regard to all mission-related information, the IPPAS team appreciated the openness displayed by those involved in discussing sensitive matters.

Throughout the mission, ASNO, ARPANSA and ANSTO personnel, and the staff of all concerned Government organisations cooperated whole-heartedly with the IPPAS team, generously giving their time, relevant information and kind hospitality. The timely provision of advance information helped to make the mission a substantial success. Moreover, the exchange of knowledge and experience between the IPPAS team members and the Australian counterparts at ASNO, ARPANSA and ANSTO was mutually beneficial.

Accordingly, the IPPAS team expresses its gratitude to ASNO, ARPANSA and ANSTO, and all those helped the mission to run smoothly and wishes to extend a particular note of thanks to their Australian hosts for such superb support.

APPENDIX I: SYNOPSIS OF RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES

Recommendations

Recommendation 1 (2017): The State should establish a national register of radioactive sources.

Recommendation 2 (2017): ASNO should develop capability to ensure effective regulatory oversight in the field of computer security of nuclear facilities.

Recommendation 3 (2017): ANSTO should complete the Configuration Management Plan and the change control process, and make sure all requested changes are submitted to a committee, reviewed, approved, developed, repaired, tested, validated, and accredited for deployment.

Recommendation 4 (2017): ANSTO should develop a maintenance procedure for all network components ———————————————————————

Suggestions

Suggestion 1 (2017): ASNO and ARPANSA should consider providing joint guidance on the appropriate application of URC and HRC for the license holders.

Suggestion 2 (2017): ASNO should consider performing a systematic staffing review of its Security Section to confirm adequacy of staffing to perform the current and emerging tasks through mapping all necessary tasks, including cyber security, against resources.

Suggestion 3 (2017): ASNO and ARPANSA should consider providing guidance on how the security zones mentioned in the PSPF can be augmented to address the recommendations and suggestions established in IAEA NSS publications.

Suggestion 4 (2017): ANSTO should consider evaluating the effectiveness of existing search procedures ———————————————————————.

Suggestion 5 (2017): The Australian Government should consider providing ANSTO with delay times and/or other performance data ———————————————————————, to assist in the effective performance evaluation of nuclear security systems and measures.

Suggestion 6 (2017): ANSTO should consider performing a systematic staffing review of the security organisation to confirm adequacy of staffing to perform the current and emerging duties, drawing special attention to those in computer security.

Suggestion 7 (2017): ANSTO should consider conducting comprehensive performance testing of the effectiveness of the security system of the ANM facility.

Suggestion 8 (2017): The relevant Competent Authority should consider providing cyber security advice on industrial control systems for Australia's critical national infrastructure, should consider advising ANSTO and other relevant entities to develop specific requirements for industrial control

systems so that recommended security requirements, best practices, and guidance do not negatively impact safe and secure operations.

Suggestion 9 (2017):

Suggestion 10 (2017):

Suggestion 11 (2017):

Suggestion 12 (2017):

Suggestion 13 (2017): ANSTO should consider ensuring that all organisational units comply with the relevant company policy/procedures to protect critical systems from infections due to media use.

Suggestion 14 (2017): ASNO should consider requiring additional NMAC activities in permits and conducting related NMAC inspections, on a graded approach, to ensure timely detection of discrepancies and unauthorised removal of nuclear material.

Suggestion 15 (2017): ASNO, ARPANSA and ANSTO should consider implementing the recommendations and suggestions provided in the IPPAS report in a timely and systematic manner.

Good practices

Good Practice 1 (2017): The regulatory body encompasses nuclear security within the Periodic Safety Review process of a research reactor, integrating nuclear safety and security in prioritization of the improvement measures assuring the future safe and secure operation of the facility.

Good Practice 2 (2017): The protective measures against threats from trusted persons with physical access to sensitive areas include a "no alone zone" function of the Electronic Access Control System.

Good Practice 3 (2017):

Good Practice 4 (2017): The Competent Authority for cyber security provides guidance to the industry through an Information Security Manual. The Competent Authority has a continuous improvement process to maintain the currency and relevance of the Information Security Manual with the changing landscape of cyber security. The Competent Authority for cyber security conducts surveys to the industry and, updates the Information Security Manual on a yearly basis, based on feedback and any new threat information.

Good Practice 5 (2017): _____

APPENDIX II: IPPAS TEAM COMPOSITION

——— **(Canada)**, Team Leader, regulatory expert

——— **(USA),** regulatory expert, physical protection expert

——— **(Germany),** regulatory expert, research reactor specialist

——— **(USA),** computer security expert

——— **(Philippine),** regulatory expert, source security specialist

——— **(Serbia),** regulatory expert, NMAC specialist

——— (**IAEA**), mission coordinator, and nuclear security and regulatory expert

——— **(Australia),** Technical and Administrative Support