INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

Mission Report: Canada

19-30 October 2015

Prepared for the Canadian Nuclear Safety Commission (CNSC)

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

This page intentionally left blank

ABBREVIATIONS

CANDU®	Canadian Deuterium Uranium
CAS	central alarm station
CATT	Canadian Adversary Testing Team
CBOP	Continuous Behavioural Observation Program
CNSC	Canadian Nuclear Safety Commission
CPPNM	*Convention on the Physical Protection of Nuclear Material* (INFCIRC/274/Rev.1)
CBRNE	Chemical, Biological, Radiological and Nuclear Emergencies
CBSA	Canada Border Services Agency
CCIRC	Canadian Cyber Incident Response Centre
CCTV	Closed Circuit Television
CIO	Chief Information Officer
CNEA	Canadian National Energy Alliance
CNL	Canadian Nuclear Laboratories
CNSC	Canadian Nuclear Safety Commission
CPPNM	*Convention on the Physical Protection of Nuclear Material*
CSA	Canadian Standards Association
CSIS	Canadian Security Intelligence Service
DBT	design basis threat
DMZ	Demilitarized Zone
DNOF	Director, Nuclear Operations and Facilities
DSC	dry storage containers
EMC	Emergency Management Centre
ENATOM	Emergency Notification and Assistance Technical Operations Manual
FERP	Federal Emergency Response Plan
FNEP	Federal Nuclear Emergency Plan
GD	Guidance Document
HEU	highly enriched uranium
IAEA	International Atomic Energy Agency
ICRP	International Commission on Radiological Protection
ICSANT	*International Convention for the Suppression of Acts of Nuclear Terrorism*
INFCIRC/225	Information Circular 225/Revision 5, *Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities*
INRA	International Nuclear Regulators Association
IPPAS	International Physical Protection Advisory Service
ITAC	Integrated Threat Assessment Centre
ITD	Inspecting Tamper Indicating Devices
LAV	light armoured vehicles
LEM	Law and Emergency Management
LEU	low enriched uranium
MDEP	Multinational Design Evaluation Program
MNR	McMaster Nuclear Reactor
MOC	Mobile Operations Centre
MoU	Memorandum of Understanding
NCA	Nuclear Cooperation Agreements
NEA	Nuclear Energy Agency
NERS	National Emergency Response System
NMAC	Nuclear Material Accountancy and Control
NMAS	Nuclear Material Accountancy System
NPP	nuclear power plant
NPT	*Non-Proliferation of Nuclear Weapons*
NRF	Nuclear Response Force

NRT	Nuclear Response Team
NSCA	Nuclear Safety and Control Act
NSD	Nuclear Security Division
NSO	Nuclear Security Officer
NSR	Nuclear Security Regulations
NSS	IAEA Nuclear Security Series
OCA	owner-controlled area
OPG	Ontario Power Generation
OPP	Ontario Provincial Police
PDCA	Plan – Do – Check – Act
PIN	Personal Identification Number
PPS	Physical Protection System
PTP	Performance Testing Program
PTZ	pan-tilt-zoom
RANET	Response and Assistance Network
RCMP	Royal Canadian Mounted Police
RD	Regulatory Document
RSE	responsible system engineer
SAT	Systematic Approach to Training
SCA	Safety and Control Area
SES	Security & Emergency Services
SMR	Security Monitoring Room
TID	Tamper Indicating Devices
TRA	threat and risk assessment
TRU	Tactical Response Unit
UFDSF	used fuel dry storage facilities
URC	unacceptable radiological consequences
WINS	World Institute for Nuclear Security
WUFDSF	Western Used Fuel Dry Storage Facility

CONTENTS

ABBREVIATIONS 3
CONTENTS 5
SUMMARY 9
I. INTRODUCTION 11
I.1. Objectives 11
I.2. Scope 12
REVIEW OF NATIONAL NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES (MODULE 1) 13
II. GOVERNMENT ORGANIZATION, ASSIGNMENTOF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION 13
II.1. Constitutional System 13
II.1.1. Legislative Branch 13
II.1.2. Executive Branch 13
II.1.3. Judicial Branch 18
II.1.4 Safety, Security and Safeguards in Canada 19
III. LEGISLATIVE AND REGULATORY FRAMEWORK 21
III.1. International Instruments 21
III.2. Laws and Secondary Legislation 22
III.2.1. Laws 22
III.2.2. Secondary legislation 24
III.2.3. Technical Guidance and other instruments 27
IV. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY 28
IV.1. Licensing/Authorization Process 29
IV.2. Inspection and Enforcement 30
IV.3. Coordination with other State Organizations That Contribute to Nuclear Security ... 32
IV.4. International Cooperation and Assistance 33
V. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT) 33
VI. RISK INFORMED APPROACH 35
VI.1. Risk Management 36
VI.2. Graded Approach 36
VI.3. Defence in Depth 36
VII. SUSTAINING THE PHYSICAL PROTECTION REGIME 37
VII.1. Security Culture 37
VII.2. Quality Assurance 38
VII.3. Confidentiality 39
VII.4. Sustainability Programme 40
VIII. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS 41
NUCLEAR FACILITY REVIEW (MODULE 2) 43
IX. BRUCE NUCLEAR GENERATING STATION 43
IX.2. Physical Protection System (PPS) 52
IX.2.1. Graded Protection and Defence in Depth 52
IX.2.2. Detection 53
IX.2.3. Access Control 55
IX.2.4. Security Monitoring Room (Central Alarm Station) 56
IX.2.5. Delay 57
IX.2.6. Response 57

X. NUCLEAR RESEARCH REACTOR AT McMASTER UNIVERSITY 58
X.1. Security Management Programme 59
X.1.1. Threat and Target Identification 59
X.1.2. Security Plan, Including Contingency Plan 59
X.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety 59
X.1.4. Security Organization 59
X.1.5. Security Staff Training and Qualification 60
X.1.6. Security Culture 61
X.1.7. Security Procedures 61
X.1.8. Confidentiality and Trustworthiness 61
X.1.9. Reporting of Nuclear Security Events 62
X.1.10. System Evaluation, including Performance Testing 62
X.1.11. Quality Assurance 62
X.1.12. Sustainability Programme 62
X.2. Physical Protection System (PPS) 62
X.2.1. Graded Protection and Defense in Depth 62
X.2.2. Detection 63
X.2.3. Access Control 63
X.2.4. Security Monitoring Room (Central Alarm Station) 63
X.2.5. Delay 64
X.2.6. Response 64
X.2.7. Radioactive Source at McMaster – Taylor Source 65
XI. WESTERN WASTE MANAGEMENT FACILITY OF ONTARIO POWER GENERATION 66
XI.1 Security Management Programme 66
XI.1.1. Threat and Target Identification 66
XI.1.2. Security Plan, Including Contingency Plan 67
XI.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety 67
XI.1.4. Security Organization 67
XI.1.5. Security Staff Training and Qualification 67
XI.1.6. Security Culture 68
XI.1.7. Security Procedures 68
XI.1.8. Confidentiality and Trustworthiness 69
XI.1.9. Reporting of Nuclear Security Events 69
XI.1.10. System Evaluation, including Performance Testing 69
XI.1.11. Quality Assurance 69
XI.1.12. Sustainability Programme 69
XI.2. Physical Protection System (PPS) 70
XI.2.1. Graded Protection and Defence in Depth 70
XI.2.2. Detection 70
XI.2.3. Access Control 70
XI.2.4. Security Monitoring Room (Central Alarm Station) 71
XI.2.5. Delay 71
XI.2.6. Response 72
TRANSPORT REVIEW (MODULE 3) 73
XII. PHYSICAL PROTECTION MEASURES FOR NUCLEAR MATERIAL DURING TRANSPORT 73
XII.1. Transport Security Legislation and Regulations 73
XII.2. Transport Security Management 74

XII.2.1. Threat and Target Identification 75
XII.2.2. Allocation of Responsibilities 75
XII.2.3. Transport Security Plan, including Contingency Plan 75
XII.2.4. Interfaces with Safety and Nuclear Material Accountancy and Control 75
XII.2.5. Security Staff Training and Qualifications 76
XII.2.6. Security Culture 76
XII.2.7. Confidentiality 76
XII.2.8. Trustworthiness 76
XII.2.9. Reporting 76
XII.2.10. System Evaluation, including Performance Testing 76
XII.2.11. Quality Assurance 77
XII.2.12. Sustainability Programme 77
XII.3. Transport Physical Protection System 77
XII.3.1. Detection 78
XII.3.2. Delay 78
XII.3.3. Response 79
SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4) 80
XIII. NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL 80
XIII.1. Assignment of Nuclear Security Responsibilities 80
XIII.1.1. State 80
XIII.1.2. Regulatory body 80
XIII.1.3. Operator, Shipper and/or Carrier 80
XIII.2. Legislative and Regulatory Framework 81
XIII.3. International Cooperation and Assistance 81
XIII.4. Identification and Assessment of Threats 82
XIII.5. Risk Based Nuclear Security Systems and Measures 82
XIII.5.1. Risk Management 83
XIII.5.2. Interface with the Safety System 83
XIII.6. Sustaining the Nuclear Security Regime 84
XIII.7. Planning and Preparedness for and Response to Nuclear Security Events 85
XIII.7.1. Trustworthiness 85
XIII.7.2. Reporting 85
XIII.8. Import and Export of Radioactive Material 85
XIV. Nordion – Kanata, Ontario 87
XIV.1. Security Management and Security Planning 87
XIV.2. Security System 88
XIV.3. Access Control 88
XIV.4. Intrusion Detection 89
XIV.5. Alarm Assessment 89
XIV.6. Emergency Power Supply 90
XIV.7. Locks and Keys 90
XIV.8. Delay 90
XIV.9. Guards and Response Forces 91
XIV.10. Communications and other Equipment 91
XIV.11. Contingency Plan 91
XIV.12. Other Observations 91
XV. SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT 92

XV.1. Transport Security Requirements and Regulations 92
XV.2. Security Management and Transport Security Plan 92
XV.3. Implemented Detection, Delay and Response Measures 92
XV.4. International Transports 93
XVI. MITIGATION AND RECOVERY OF NUCLEAR AND OTHER RADIOACTIVE MATERIALS 93
XVI.1. Location and Recovery of Missing/Stolen Material 93
XVI.2. Measures to Mitigate/Minimize Radiological Consequences of Sabotage 94
XVII. COMPUTER SECURITY STATE LEVEL REVIEW 95
XVII.1. Legal and Regulatory Framework 95
XVII.2. Roles and Responsibilities of Competent Authority 98
ACKNOWLEDGEMENTS 107
Appendix I: Synopsis of Recommendations, Suggestions and Good Practices 108
Appendix II: IPPAS team Composition 114

SUMMARY

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) mission conducted in Canada from 19 to 30 October 2015. This is the 68th IPPAS mission conducted by the IAEA since the introduction of this service in 1995. Canada is the 43rd country to host an IPPAS mission. Canada is one of the first countries to request that an IPPAS mission include a comprehensive review of the national nuclear security regime, including all five IPPAS modules.

In preparation for the mission, a national workshop on IPPAS was conducted from 4 to 5 May, 2015 followed by a preparatory meeting on 6 May, 2015 in Ottawa, during which the arrangements for the mission were discussed and agreed upon.

The objectives of the IPPAS mission were to review the following: the current status of the national nuclear security regime of nuclear and other radioactive material and associated facilities and activities; review the implementation of the nuclear security measures at Bruce Power Nuclear Generating Station, Western Used Fuel Dry Storage Facility operated by Ontario Power Generation, Nordion Kanata nuclear substance processing facility (hereafter referred to as Nordion) and the McMaster University Nuclear Reactor (MNR); compare the procedures and practices of Canada with the *Convention on the Physical Protection of Nuclear Material* (*CPPNM*) and its 2005 *Amendment*; *Code of Conduct on the Safety and Security of Radioactive Sources; IAEA Nuclear Security Series (NSS) No. 20, Objective and Essential Elements of a State's Nuclear Security Regime; IAEA NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5); IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities,* and with other relevant IAEA NSS documents; provide recommendations and suggestions for continued improvement of nuclear security; and identify good practices.

The scope of the mission covered all five IPPAS modules, including National Review of Nuclear Security Regime for Nuclear Material and Nuclear Facilities (Module 1), Nuclear Facility Review (Module 2), Transport Review (Module 3), Security of Radioactive Material, Associated Facilities and Associated Activities (Module 4) and Computer Security Review (Module 5). The issues related to nuclear security interfaces with nuclear material accountancy and control, and safety were also addressed during the mission.

For this IPPAS mission, the IAEA assembled a ten-person team comprising experts from nine nations and the IAEA. The experts have broad expertise and extensive experience in nuclear legislation, regulatory oversight, physical protection system design, implementation and assessment, including computer security. During the mission, the IPPAS team interacted with key management and personnel from the Canadian Nuclear Safety Commission (CNSC) as well as management and staff from the facilities visited.

It was apparent to the IPPAS team that a significant amount of time and effort was invested by the CNSC and other participants in the preparation and conduct of the mission. The CNSC provided the IAEA and the IPPAS team members with an advanced information package consisting of relevant information related to Canada's legislative and regulatory framework, roles and responsibilities of the competent authorities and other Canadian organisations involved in nuclear security, as well as information on nuclear facilities and activities. The relevant Canadian legal and regulatory documents on nuclear security and a nuclear security self-assessment were also included in the advanced information package.

The IPPAS team recognized that Canada has established and maintains a robust and comprehensive nuclear security infrastructure and that the CNSC assures licensees' compliance with regulatory requirements. It is important to note that Canada is adhering and contributing to all international instruments relevant to nuclear security and that Canada's nuclear security legislation is continually being updated and enhanced.

The IPPAS team also noted that the CNSC encourages the adoption of good nuclear security practices which exceed current regulatory requirements. This is most obvious in the fields of transport security, computer security, emergency preparedness and security response. Nuclear security in Canada benefits from a mature, well-balanced and comprehensive national intelligence framework supported by national and international security and intelligence partnerships.

Good practice is also evident through the systematic approach applied to the evaluation of requests for export. Indeed, the IPPAS team noted that Canada pays particular attention to end-use and end-user certificates when considering the potential security implications of any such transaction.

The IPPAS team was assured that both the CNSC and nuclear licensees continue to identify opportunities to enhance current security practices. Regulatory changes to frame these new opportunities are evolving; particularly in the area of computer security, which remains a key priority. In this regard, the working group engagements between Canadian civil nuclear licensees for the purposes of ensuring wide understanding of computer based threats and vulnerabilities and the support of the Canadian Cyber Incident Response Centre (CCIRC) is particularly worthy of praise.

Notwithstanding these assurances, the IPPAS team acknowledges there are areas which should be addressed if current levels of regulatory assurances for security are to be sustained and developed. Specifically, although an imbalance between the relative importance of security and safety is slowly being addressed, more work needs to be done to ensure there is a wider acceptance that the relative merits of these specialisations are closely aligned. Such improvements are likely to be most effectively delivered through a commitment to promote the importance of Nuclear Security Culture both within the CNSC and amongst its licensees.

A total of 3 Recommendations and 30 Suggestions were provided which could enhance nuclear security. In addition a total of 21 Good practices were identified during the mission, which if shared, could benefit other Member States in enhancing nuclear security.

In conclusion, the IPPAS team assesses Canada has a mature and well-established nuclear security regime which has been enhanced significantly in recent years.

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

I. INTRODUCTION

The International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) programme is a fundamental part of the IAEA's efforts to assist Member States to establish and maintain an effective nuclear security regime for nuclear and other radioactive material, associated facilities and associated activities. The IPPAS is offered to Member States, upon request, as peer review and assessment of their State's nuclear security regime, including a national level review of the legal and regulatory framework, and implementation measures and procedures in place to execute this framework at facilities and during transport. Relevant international instruments and the IAEA Nuclear Security Series (NSS) guidance are used as the basis for IPPAS assessment.

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) mission conducted in Canada from 19 to 30 October 2015. This is the 68th IPPAS mission conducted by the IAEA since the introduction of this service in 1995. Canada is the 43rd country to host an IPPAS Mission.

The Prime Minister of Canada announced during the third Nuclear Security Summit held in the Netherlands on 24 and 25 March, 2014 that Canada would host an IPPAS mission in 2015. On 29 January 2014, the Department of Foreign Affairs, Trade and Development of Canada requested that the IAEA conduct an IPPAS mission to assess the nation's nuclear security regime for nuclear and other radioactive material and associated facilities and activities. The Canadian Nuclear Safety Commission (CNSC) has been identified as the host country's organization for coordinating the preparation and conduct of the mission.

In preparation for the mission, a national workshop on IPPAS was conducted from 4 to 5 May, 2015 followed by a preparatory meeting on 6 May, 2015 in Ottawa during which, the arrangements for the mission were discussed and agreed upon.

For this IPPAS mission, the IAEA assembled a ten-person team (see Appendix II) comprising experts from nine nations and the IAEA. The experts have broad experience in nuclear legislation, regulatory oversight, physical protection system design, implementation and assessment, including computer security.

I.1. Objectives

The objectives of the IPPAS mission were to:

- review the current status of the national nuclear security regime of nuclear and other radioactive material and associated facilities and activities;
- review the implementation of the nuclear security measures at Bruce Power Nuclear Generating Station, Western Used Fuel Dry Storage Facility, McMaster University Nuclear Reactor and Nordion;
- compare the procedures and practices of Canada with the *Convention on the Physical Protection of Nuclear Material* (*CPPNM*) and its 2005 *Amendment*; *Code of Conduct on the Safety and Security of Radioactive Sources; IAEA Nuclear Security Series (NSS) No. 20, Objective and Essential Elements of a State's Nuclear Security Regime; IAEA NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5); IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities;* and with other relevant IAEA NSS documents;
- provide recommendations and suggestions for continued improvement of nuclear security;
- identify good practices, which, if shared, could benefit other Member States in enhancing nuclear security.

I.2. Scope

The scope of the mission covered all five IPPAS modules, including National Review of Nuclear Security Regime for Nuclear Material and Nuclear Facilities (Module 1), Nuclear Facility Review (Module 2), Transport Review (Module 3), Security of Radioactive Material, Associated Facilities and Associated Activities (Module 4) and Computer Security Review (Module 5). The issues related to nuclear security interfaces with nuclear material accounting and control, and safety were also addressed during the mission.

The CNSC provided the IAEA and the IPPAS team members with an advanced information package consisting of relevant information related to Canada's legislative and regulatory framework, roles and responsibilities of the competent authority and other Canadian organisations involved in nuclear security, as well as information on nuclear facilities and activities. The relevant Canadian legal and regulatory documents on nuclear security and the nuclear security self-assessment were also included in an advanced information package. The advanced information package did not include any sensitive or confidential information.

During the mission, the team gathered additional information on the current legal and regulatory structure through briefings and interviews with Government officials representing the CNSC and other Canadian authorities. Facility visits were also made to Bruce Power Nuclear Generating Station, Western Used Fuel Dry Storage Facility, McMaster University Nuclear Reactor and Nordion where the team observed the implementation of physical protection practices and held discussions with facility personnel. Meetings with staff of the CNSC, and the facility visits, also provided opportunities for informal exchange of information on nuclear security practices used in other countries and the opportunity to discuss the technical aspects of implementing physical protection systems.

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

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

II. GOVERNMENT ORGANIZATION, ASSIGNMENTOF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION

II.1. Constitutional System

Canada is a constitutional monarchy and a parliamentary democracy. The government system consists of executive, legislative and judicial branches. Additionally, Canada's government consists of three levels: 1) federal; 2) provincial; 3) municipal.

Under the Constitution Act (1982), nuclear power is the responsibility of the federal government. From the point of view of nuclear security, it is important to note that:
1) The federal government is also responsible for areas such as criminal law and national defence;
2) The provincial governments deal with areas such as health care and emergency preparedness, however emergency preparedness is a responsibility shared with the federal government. It is important to note that in the event of a conflict on the matter of shared jurisdiction, the federal law would be paramount;
3) The municipal governments have responsibilities such as for the local police.

II.1.1. Legislative Branch

The legislative power is vested in the Parliament of Canada pursuant to section 17 of the Constitution Act of 1867.

Under the Constitution Act, 1867 legislative powers are divided between the federal Parliament and provincial governments, and enumerated as belonging to one or the other. For matters not specifically enumerated such as nuclear, the Act authorizes the federal Parliament to make laws for the "peace, order and good government of Canada." Under this authority and as a result of Parliament's enactment of s.71 of the Nuclear Safety and Control Act, nuclear has been assigned as a matter of federal legislative authority.

II.1.2. Executive Branch

As Canada is also a constitutional monarchy, pursuant to section 9 of the Constitution Act of 1867, the executive government and authority of and over Canada is vested in the Queen. The executive function is carried out by the Governor in Council, which is the Governor General acting with, and on the advice of, the Prime Minister and the Cabinet.

Relevant functions of the *Governor in Council* are the following:
1) approving the regulations made by the CNSC (subsection 44(1) of the NSCA);
2) making regulations considered necessary for carrying out the purposes of the NSCA (subsection 44(5) of the Nuclear Safety and Control Act (NSCA));
3) appointing and dismissing permanent and temporary members of the CNSC, including the designation of one of them as the President (section 10 of the NSCA);

4) issue to the CNSC binding directives of general application on broad policy matters with respect to the objects of the CNSC (section 19 of the NSCA);
5) by order, excluding the Department of National Defence or the Canadian Forces from the application of the NSCA or any regulations made pursuant to this Act, to the extent and under the conditions specified in the order (section 5 of the NSCA).

The relevant departments in the nuclear security area are:

1) *Natural Resources Canada*.
The department is established under the Department of Natural Resources Act. The Minister of Natural Resources, appointed by commission under the Great Seal, presides over the department. Pursuant to subsection 5(a) of the Department of Natural Resources Act (DNRA), the powers, duties and functions of the Minister include all matters over which Parliament has jurisdiction, not by law assigned to any other department, board or agency of the Government of Canada, relating to natural resources. As natural resources are defined, pursuant to section 2 of the DNRA as "mines, minerals and other non-renewable resources, energy, including energy developed from water, and forest resources", this definition also encompasses the area of nuclear energy. Pursuant to section 6 of the Department of Natural Resources Act, while exercising his powers, duties and functions, the Minister shall have regard, notably, to the sustainable development of Canada's natural resources and their integrated management, assist in the development and promotion of Canadian scientific and technological capabilities and participates in the development and application of codes and standards for technical surveys and natural resources products, promote cooperation with the governments of the provinces and with non-governmental organizations in Canada, and participate in the promotion of cooperation with the governments of other countries and with international organizations.

According to the information provided to the IPPAS team, both the CNSC and Atomic Energy of Canada Limited (which is a federal Crown corporation, responsible for the long term, contractual arrangement with the Canadian National Energy Alliance (CNEA) for the management and operation of Canadian Nuclear Laboratories (CNL)) report to Parliament through annual reports submitted to the Minister of Natural Resources. In the case of CNSC's annual report this procedure is embedded in the section 72 of the NSCA. Additionally, pursuant to subsection 12(4) of the NSCA, subject to regulations made pursuant to paragraph 44(1)(d), the President [of the CNSC] shall make such reports to the Minister of Natural Resources as the Minister may require concerning the general administration and management of the affairs of the CNSC and such of these reports as the Minister may direct shall form part of the report referred to in section 72. From the point of view of the relation of these provisions to the NSS No. 13 para 3.18, stating that "the State's competent authority should have clearly defined legal status and be independent from applicants/operators/shippers/carriers and have the legal authority to enable it to perform its responsibilities and functions effectively", it was confirmed to the IPPAS team that the arrangements mentioned above are merely formal/administrative and do not result in governmental control over the activities of the CNSC.

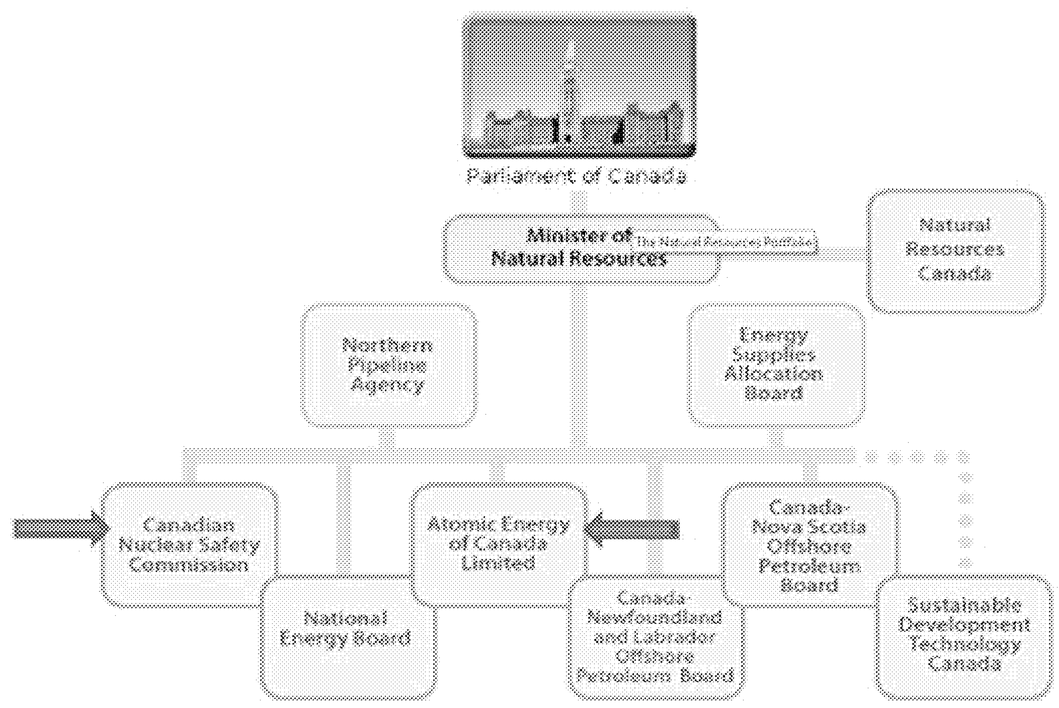

Figure 1. Organizational chart in relation to Department of Natural Resources Canada

2) *Public Safety Canada*

Pursuant to section 3 of the Emergency Management Act, the Minister of Public Safety and Emergency Preparedness is responsible for exercising leadership relating to emergency management in Canada by coordinating, among government institutions and in cooperation with the provinces and other entities, emergency management activities. Pursuant to section 4, while exercising this mandate, the Minister's responsibilities include:

a) establishing policies, programs and other measures respecting the preparation, maintenance, testing and implementation by a government institution of emergency management plans;

b) providing advice to government institutions respecting the preparation, maintenance, testing and implementation of emergency management plans;

c) analysing and evaluating emergency management plans prepared by government institutions;

d) monitoring potential, imminent and actual emergencies and advising other ministers accordingly;

e) coordinating the Government of Canada's response to an emergency;

f) coordinating the activities of government institutions relating to emergency management with those of the provinces – and supporting the emergency management activities of the provinces – and through the provinces, those of local authorities;

g) establishing arrangements with each province whereby any consultation with its lieutenant governor in council with respect to a declaration of an emergency under an Act of Parliament may be carried out effectively;

h) coordinating the provision of assistance to a province in respect of a provincial emergency, other than the provision of financial assistance and the calling out of the Canadian Forces for service in aid of the civil power under Part VI of the National Defence Act;

i) providing assistance other than financial assistance to a province if the province requests it;

j) providing financial assistance to a province if (i) a provincial emergency in the province has been declared to be of concern to the federal government under section 7, (ii) the Minister is authorized under that section to provide the assistance, and (iii) the province has requested the assistance; and other responsibilities (paragraphs 4(l)(k) to (r) of section 4 of the Emergency Management Act).

According to the information provided for the IPPAS team, the Minister of Public Safety and Emergency Preparedness, in consultation with the Minister of Foreign Affairs, is responsible for the Canada's Counter-Terrorism Strategy's implementation.

According to the information provided for the IPPAS team, Public Safety Canada works with federal agencies with security nexus listed below, that are a part of a single portfolio related to public safety:

1) The Canada Border Services Agency (CBSA) manages Canada's borders by enforcing Canadian laws governing trade and travel, as well as international agreements and conventions, including seizing goods that are non-compliant with export laws and regulations. According to the information provided to the IPPAS team, their mandate includes responsibilities concerning the location and recovery of missing nuclear and radioactive materials at the border after they are notified about the situation;

2) The Canadian Security Intelligence Service (CSIS), in accordance with the Canadian Security Intelligence Service Act (including its amendment – the Protection of Canada from Terrorist Act) investigates and reports on activities that may pose a threat to the security of Canada and produces intelligence. CSIS also provides security assessments, on request, to all federal departments and agencies;

3) The Royal Canadian Mounted Police (RCMP) enforces Canadian laws, prevents crime and maintains peace, order and security. The RCMP has prime responsibility for the investigation of offences involving national security. According to the information provided to the IPPAS team, the local police would be notified about missing nuclear and radioactive materials by a CNSC licensee and would be responsible for location and recovery of the materials. The licensee would provide any assistance (e.g. radiation protection expertise).

3) *Transport Canada.*
Pursuant to the Transportation of Dangerous Goods Act and according to the Memorandum of Understanding between Transport Canada (Transport Dangerous Goods Directorate) and the CNSC, Transport Canada is responsible for:

1) regulating the handling, offering for transport, transport and import of dangerous goods (pursuant to the Transportation of Dangerous Goods Act, nuclear substances, within the meaning of the NSCA, that are radioactive, fall within class 7 of dangerous goods);

2) providing consultations to CNSC, which is responsible for regulating all aspects of physical security of nuclear substances and prescribed equipment, as defined under NSCA and its regulations, with regard to such regulation;

3) consultation on other issues related to class 7 of dangerous goods.
According to the information provided for the IPPAS team, in broad terms the role of Transport Canada with respect to the nuclear sector is to promote public safety during the transportation of dangerous goods and the Transportation of Dangerous Goods Directorate is the leading source of regulation, information and advice on dangerous goods transport for the public, industry and government employees.

4) *Health Canada.*
Pursuant to subsection 4(1) of the Department of Health Act, the powers, duties and functions of the Minister of Health extends to and includes all matters over which Parliament has jurisdiction relating to the promotion and preservation of the health of the people of Canada not by law assigned to any other department, board or agency of the Government of Canada.

According to the information provided to the IPPAS team, Health Canada, together with the CNSC, is a national competent authority for the Convention on Early Notification of a Nuclear Accident, the Emergency Communications Emergency Notification and the Assistance Technical Operations Manual (ENATOM), the Convention on Assistance in Case of a Nuclear Accident or Radiological Emergency and the IAEA Response and Assistance Network (RANET).

In the event that provincial or territorial authorities require assistance from the federal government, Health Canada coordinates federal actions in support of provinces and territories by activating the Federal Nuclear Emergency Plan.

5) *Foreign Affairs, Trade and Development Canada.*
Pursuant to subsection 10(1) of the Department of Foreign Affairs, Trade and Development Act, the powers, duties and functions of the Minister of Foreign Affairs, presiding over the Department of Foreign Affairs, Trade and Development, extends to and includes all matters over which Parliament has jurisdiction, not by law assigned to any other department, board or agency of the Government of Canada, relating to the conduct of the external affairs of Canada. According to the information provided to the IPPAS team, the Department of Foreign Affairs promotes bilateral and multilateral nuclear cooperation and safety, and the implementation in Canada and abroad of key non-proliferation and disarmament agreements and enhances security and well-being by promoting the peaceful and safe use of chemical and nuclear technologies, e.g., the Department is responsible of ensuring compliance with international commitments such as the Comprehensive Nuclear Test Ban Treaty and the Chemical Weapons Convention.

In summary, it should be noted that the mandates of the relevant departments are defined broadly in the Acts establishing a particular department and, as the IPPAS team was informed, the participation of the relevant governmental departments in the nuclear security regime is usually arising from their general mandate, which is a usual practice in Canada.

Additionally, as the IPPAS team was informed, in the instance of any shared areas of jurisdiction or areas needing clarification, Memorandums of Understanding (MoU) and Administrative Arrangements are usually concluded between relevant departments, agencies, etc. MoUs are non-legally binding documents, listing functions and responsibilities of relevant authorities in particular areas, however participants endeavour to respect the undertaken responsibilities in good faith. The CNSC has, for example, concluded MoUs with the following governmental departments/agencies, with respect to nuclear security: Transport Canada (among other areas, deals with transportation of class 7 dangerous goods) and Health Canada (concluded in respect of cooperation the following areas: provision of standards, calibration and independent testing, the National Dose Registry, investigations, tests and studies, environmental assessments, radiological and nuclear emergencies and incidents and licencing and certification of medical devices), which clarify the delineation of responsibilities and functions between the CNSC and the aforementioned governmental departments. However, according to the information provided to the IPPAS team, MoUs between the CNSC and other governmental departments are not directly connected to clarification of functions in the area of nuclear security.

That being said, the practice mentioned above (i.e. participation of the relevant governmental departments in the nuclear security regime to be arising from their general mandate only) may raise problems while ensuring adherence to the provision of Nuclear Security Fundamentals, IAEA NSS. 20, Essential Element 2: Identification and definition of Nuclear Security Responsibilities: “Nuclear security responsibilities of competent authorities designated by the State, as described in Essential Element 3, including regulatory bodies and those competent authorities related to border control and law enforcement, and the responsibilities for all authorized persons, are clearly identified and defined. Provisions are identified and defined for appropriate integration and coordination of responsibilities within the nuclear security regime, as well as for the State’s oversight to ensure the continued appropriateness of the nuclear security responsibilities”.

Suggestion: The CNSC should consider Memorandums of Understanding between itself and other Canadian Government departments or agencies, specifically focused on nuclear security responsibilities and functions and (or) consider revising the current MoUs.

It is also important to mention the role of the Treasury Board (as one of the "central" agencies in Canada), which issues standards and guidelines for protecting information and applying appropriate clearances, which are mandatory for governmental departments and agencies.

According to the provided information, the network of the international and multilateral cooperation includes such organizations as IAEA, Nuclear Energy Agency (NEA, OECD), Zangger (Nuclear exporters) Committee, G7 Nuclear Safety and Security Group, International Commission on Radiological Protection (ICRP), International Nuclear Regulators Association (INRA), CANDU Senior Regulators, Nuclear Suppliers Group and Multinational Design Evaluation Program (MDEP). Additionally, pursuant to paragraph 21(1)(a) of the NSCA, the CNSC, in order to attain its objects, may enter into arrangements, including an arrangement to provide training, with any person, any department or agency of the Government of Canada or of a province, any regulatory agency or department of a foreign government or any international agency.

According to the information provided to the IPPAS team, concerning bilateral cooperation on import and export, agreements are concluded on two levels. On the Governmental level, Nuclear Cooperation Agreements (NCAs) are concluded to establish reciprocal obligations designed to minimize risks of proliferation associated with nuclear transfers. To implement the NCAs on the regulator's level, Administrative Arrangements are concluded. Administrative Arrangements can also be concluded with other regulatory bodies or designated implementing authorities, to specify arrangements in other areas (the IPPAS team was provided with the example of an agreement specifying Arrangements under the IAEA Code of Conduct on the Safety and Security of Radioactive Sources).

Taking into account the information mentioned above, it can be concluded that adequate arrangements for international cooperation and assistance are provided in Canada's national legislation.

II.1.3. Judicial Branch

The court system of Canada consists of the Supreme Court of Canada, as well as federal, provincial and territorial courts. There are also Court Martial Appeal Court and Military Courts.

The Supreme Court of Canada is the final court of appeal. The Supreme Court of Canada hears appeals from decisions of the appeal courts of all the provinces, territories and the Federal Court of Appeal. Supreme Court judgments are final. The Supreme Court of Canada also makes decisions on important questions about the Constitution and controversial or complicated areas of private and public law and provides an opinion on important legal questions upon the request of government.

The other federal courts are:
1) *The Federal Court* (specializes in areas such as intellectual property, maritime law, federal–provincial disputes and civil cases related to terrorism);
2) *The Tax Court* (specializes in hearing appeals from tax assessments);
3) *The Federal Court of Appeal* (reviews the decisions of the Federal Court and the Tax Court).

On the *provincial level* the court system usually consists of the following levels of courts:
1) provincial and territorial (or lower) courts (try most criminal offences, family matters);
2) superior courts (deal with the most serious criminal and most civil cases and have the power to review the decisions of the provincial and territorial courts, in most cases), which are divided into trial level and appeal level.

Provincial courts may also include specialized courts, such as youth courts, family courts, and small claims courts.

There are also *administrative boards and tribunals*, which deal with disputes over the interpretation and application of laws and regulations. Decisions of administrative boards and tribunals may be reviewed by superior courts.

It is important to note that, pursuant to subsection 65.14(5) of the NSCA and section 18.1 of the Federal Courts Act, CNSC's decisions are not appealable, and they can only be reviewed by the Federal Court. Additionally, pursuant to subsection 20(8) of NSCA, any decision or order of the CNSC may, for the purposes of enforcement, be made a rule or decree of the Federal Court or of a superior court of a province and may be enforced in like manner as a rule, order or decree of that court.

II.1.4 Safety, Security and Safeguards in Canada

Pursuant to section 8 of the NSCA, the CNSC was established with the objects of regulation of safety, security and safeguards delegated to it pursuant to section 9 of the NSCA. The objects of the CNSC are, pursuant to section 9 of the NSCA, the following:

a) to regulate the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information in order to (i) prevent unreasonable risk, to the environment and to the health and safety of persons, associated with that development, production, possession or use, (ii) prevent unreasonable risk to national security associated with that development, production, possession or use, and (iii) achieve conformity with measures of control and international obligations to which Canada has agreed; and

b) to disseminate objective scientific, technical and regulatory information to the public concerning the activities of the CNSC and the effects, on the environment and on the health and safety of persons, of the development, production, possession and use referred to in the paragraph above.

The IPPAS team noted substantial integration within the CNSC across the safety and security interface.

Suggestion: The CNSC should consider the enhancement of policies and processes which elevate the relative importance of security to ensure it equates with that of safety.

The CNSC is Canada's competent authority with respect to nuclear safeguards as set out in Agreement between the Government of Canada and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-proliferation of Nuclear Weapons (under the INFCIRC/153) and the Protocol Additional to the Safeguards Agreement concluded between Canada and the International Atomic Energy Agency (the Additional Protocol is in force since 2000). It is worthwhile noting that the responsibilities of the licensees are also usually embedded in the licence conditions, as a general requirement for the licensee to "implement and maintain the safeguards program". One important element of Safeguards is NMAC (Nuclear Material Accounting and Control), that is regulated by the CNSC. NSS No. 13 recognizes the importance of NMAC for nuclear security in para 3.36:

"When considering the threat, due attention should be paid to insiders. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The physical protection system should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of nuclear material by an insider".

The IAEA has recently published the implementing guide NSS No. 25-G "Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities". In this document, importance of NMAC system for nuclear security purposes, especially against the insider adversary threat, has been recognized.

Basis: NSS No. 25-G, para 3.11:
"The criteria and performance requirements for an NMAC system are established in the overall context of nuclear security and are especially useful to assess the nuclear security system against the insider threat. The criteria should address the different types of nuclear material and the timeframes for detection of unauthorized removal of nuclear material".

Suggestion: The CNSC should consider reviewing the criteria and performance requirements for an NMAC system for nuclear security purposes to detect an attempt of unauthorized removal (both abrupt and protracted theft), to improve measures against the insider threat.

Pursuant to paragraph 24(4)(b) of the NSCA, no license shall be issued, renewed, amended or replaced – and no authorization to transfer one given – unless, in the opinion of the CNSC, the applicant or, in the case of an application for an authorization to transfer the license, the transferee will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed. Pursuant to section 12(1.c) of the General Nuclear Safety and Control Regulations the licensees are obligated to maintain the security of all nuclear facilities and nuclear substances. The provisions mentioned above provide for assurance that prime responsibility for safety and security rests with the licensee.

Taking into consideration:

- the purpose of the NSCA, as defined in it's section 3, is "to provide for (a) the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information; and (b) the implementation in Canada of measures to which Canada has agreed respecting international control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive devices";

- that the CNSC has a broad power to make regulations generally as it considers necessary for carrying out the purposes of the NSCA and to assist the Commission in attaining its objects (paragraph 44(1)(w)), also to authorize and inspect the nuclear-related activities and impose enforcement actions;

- the respective powers, duties and responsibilities of other governmental departments and agencies;

- the international conventions that Canada is a party to;

- that Canada has ratified the Amendment to the Convention on the Physical Protection of Nuclear Material as well as the International Convention for the Suppression of Acts of Nuclear Terrorism, by amending the Criminal Code to create new offences related to nuclear terrorism;

it may be concluded that Canada's legislation provides for sufficient basis of implementation of relevant provisions of the CPPNM and the Amendment to the CPPNM.

III. LEGISLATIVE AND REGULATORY FRAMEWORK

III.1. International Instruments

Canada is a party to the following international instruments relevant to nuclear security:

- *the Convention on the Physical Protection of Nuclear Material (CPPNM)*. Canada ratified the CPPNM and became a State Party in 1986. Canada also ratified the *Amendment to the CPPNM* on December 3rd, 2013. CNSC is a competent authority under the CPPNM (according to information provided by the country CNSC is designated as a competent authority as a part of their general mandate and as per declaration to the IAEA). The measures contemplated in the CPPNM and the Amendment to the CPPNM are introduced into the national legal system through the Criminal Code, the NSCA and the Nuclear Security Regulations.

- *the International Convention for the Suppression of Acts of Nuclear Terrorism* (ICSANT). The ICSANT was ratified by Canada on November 21st, 2013. The amendments to the Criminal Code (also referred to as *the Nuclear Terrorism Act*) introduces the relevant provisions on criminalization of acts stipulated in Article 2 of ICSANT.

- *the Treaty on Non-Proliferation of Nuclear Weapons* (NPT). The CNSC is competent authority with respect to nuclear safeguards as set out in Agreement between the Government of Canada and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-proliferation of Nuclear Weapons (under the INFCIRC/153) and the Protocol Additional to the Safeguards Agreement concluded between Canada and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-proliferation of Nuclear Weapons (the Additional Protocol is in force since 2000).

- *Convention on Early Notification of a Nuclear Accident* and *Convention on Assistance in Case of a Nuclear Accident or Radiological Emergency*. According to the information provided for the IPPAS team, Health Canada together with CNSC is a national competent authority for these conventions.

Canada is also a party to the Convention on Nuclear Safety and Joint Convention on Spent Fuel Management and Radioactive Waste Management.

Considering *Security Council resolutions*, according to the information provided for the IPPAS team, Canada has submitted the reports pursuant to the Security Council resolutions 1540, in 2004, 2006 and 2008 and Canada has also submitted a Summary Action Plan to the 1540 Committee in August 2010, and is in the process of updating its National Action Plan on 1540 implementation. According to the information provided to the IPPAS team, the Department of Foreign Affairs, Trade and Development would be responsible for gathering the information from relevant governmental departments and agencies (e.g. CNSC) and providing the report.

IAEA's documents are not directly referenced in the legislation, however according to the information provided by the country they are used as a basis while drafting legislation and in some cases they are referred to in the licence.

According to the information provided to the IPPAS team, Canada has provided political commitment to both the IAEA Code of Conduct on the Safety and Security of Radioactive Sources and the Guidance on the Import and Export of Radioactive Sources.

III.2. Laws and Secondary Legislation

III.2.1. Laws

Laws establishing the overall duties and responsibilities of relevant government departments are the following:, Department of Natural Resources Act, Emergency Management Act (establishes powers, responsibilities and functions of the Minister of Public Safety and Emergency Preparedness), Canadian Security Intelligence Service Act, Transportation of Dangerous Goods Act, Department of Foreign Affairs, Trade and Development Act, etc. (also see II.1.2).

Laws explicitly dealing with relations in the area of nuclear safety, security and safeguards are listed below.

Nuclear Safety and Control Act (NSCA)

The main law regulating nuclear energy in Canada is the Nuclear Safety and Control Act (NSCA). It regulates all nuclear-related facilities and activities. Pursuant to section 3 of the NSCA, the purpose of the act is to provide for: a) the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information; b) the implementation in Canada of measures to which Canada has agreed respecting international control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive.

The NSCA provides for all essential elements (and (or) their basis) of the legal and regulatory framework as required by Amendment to the CPPNM Fundamental Principle C, i.e. provisions on:
1) establishing the competent authority – CNSC (section 8);
2) applicable physical protection requirements (section 44);
3) authorization regime (sections 24–26);
4) regulatory inspections (section 30);
5) enforcement measures (e.g. sections 48–51).

The NSCA applies to all government entities with the exemption of Canada's Department of National Defence (DND) and the Canadian Armed Forces (CAF) by the order of the Governor in Council (Order-In-Council PC 2000-1421 dated 13th of September 2000).

Criminal Code

Criminal Code (as amended by the Nuclear Terrorism act) criminalizes certain acts as required by the CPPNM and the Amendment to the CPPNM and the ICSANT. Sections 82.3 to 82.6 of the Code cover offences that are related to nuclear facilities, nuclear and radioactive materials and devices. Section 82.2 stipulates that "device" means any of the following: a) a nuclear explosive device; b) a device that disperses radioactive material; c) a device that emits ionizing radiation and that is capable of causing death, serious bodily harm or substantial damage to property or the environment. The Criminal Code also includes definitions for nuclear facility, nuclear and radioactive material.

Section 83.01 (v), within the list of activities described as terrorist activities, includes "the offences referred to in subsection 7(2.21) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980, as amended by the Amendment to the Convention on the Physical Protection of Nuclear Material, done at Vienna on July 8, 2005 and the International Convention for the Suppression of Acts of Nuclear Terrorism, done at New York on

September 14, 2005". Offences related to terrorist activities are further criminalized in respective sections (e.g. carrying out terrorist activity, facilitating terrorist activity, etc.).

Transportation of Dangerous Goods Act

The transportation of dangerous products by air, marine, rail and road is regulated under this Act. Pursuant to this Act, nuclear substances, within the meaning of the NSCA, that are radioactive, fall within class 7 of dangerous goods. Pursuant to section 7.3(1) of the Act, no prescribed person shall import, offer for transport, handle or transport dangerous goods in a quantity or concentration that is specified by regulation – or that is within a range of quantities or concentrations that is specified by regulation – before the person has undergone security training in accordance with the regulations, has a security plan and has implemented the plan in accordance with the regulations. Pursuant to section 7.3(2) of the Transportation of Dangerous Goods Act, "the security plan shall, in accordance with the regulations, set out measures to prevent the dangerous goods from being stolen or otherwise unlawfully interfered with in the course of the importing, offering for transport, handling or transporting". Additionally, the Act provides the inspectors designated by the Minister of Transport with variety of powers to verify the compliance with this Act, including, e.g., to stop any means of transport for which the inspector is designated and enter and inspect any place, or any such means of transport, if the inspector believes on reasonable grounds that in or on the place or means of transport there are dangerous goods being offered for transport, handled or transported. The designated inspectors may also remove the dangerous goods or direct the person to do anything else or refrain from doing anything that might impede the prevention of the release of dangerous goods or the reduction of the danger (section 19(1) of the Transportation of Dangerous Goods Act). Additionally, with respect of class 7 of dangerous goods (nuclear substances, within the meaning of the NSCA, that are radioactive), pursuant to section 27 of the Transportation of Dangerous Goods Act, the Minister of Transport is empowered to make regulations related to transportation of the dangerous goods, i.e. regulations generally for carrying out the purposes of the Transportation of Dangerous Goods Act.

Access to Information Act and *Security of Information Act* are benchmark documents in the area of information security. Access to Information Act sets provisions on the public's right of access to information in records under the control of a government institution and describes types of information which shall or may be refused to be provided. The latter includes information, which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities (including sabotage, activities directed toward the commission of terrorist acts, including hijacking, in or against Canada or foreign states, etc.) (sections 15(1) and (2)). Security of Information Act provides for acts that constitute an offence in the area of information security. Additionally section 48(b) of the NSCA stipulates that every person commits an offence who discloses prescribed information, except pursuant to the regulations. Pursuant to section 21(1) of the General Nuclear Safety and Control Regulations, prescribed information (for the purposes of the NSCA) is: (a) a nuclear substance that is required for the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device, including the properties of the nuclear substance; (b) the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device; (c) the security arrangements, security equipment, security systems and security procedures established by a licensee in accordance with the NSCA, the regulations made under the NSCA or the licence, and any incident relating to security; and (d) the route or schedule for the transport of Category I, II or III nuclear material, as defined in section 1 of the Nuclear Security Regulations.

This information security regime is supplemented by Treasury Board's documents, which include Policy of the Government Security, standards issued under this Policy, that include requirements for information and identity security, individual security screening, physical security, information technology security, etc. (e.g. Security Organization and Administration Standard, setting requirements for security of information, such as levels of classification of the information and

Personnel Screening Standard). The Policy, directives and standards are mandatory. The Treasury Board also issues guidelines and tools, which are voluntary. The Acts and Treasury Board documents are applicable to the CNSC and other governmental agencies and through the REGDOC 2.12.2 Site Access Security Clearance, which is a licence condition for the licensees to adhere to while handling the sensitive information provided for them by the CNSC (e.g. DBT).

III.2.2. Secondary legislation

Secondary legislation for the nuclear-related facilities and activities consists of regulations, emergency orders of CNSC and orders of Governor in Council.

Regulations

Pursuant to section 44(1) of the Nuclear Safety and Control Act (NSCA), CNSC, with the approval of the Governor in Council, may make regulations. The areas of such regulations are provided in subsections a–w of section 44(1), including regulations respecting measures to ensure the maintenance of national security and compliance with Canada's international obligations in the development, production and use of nuclear energy and the production, use, possession, packaging, transport, storage and disposal of nuclear substances, prescribed equipment and prescribed information. Pursuant to section 44(1.w) of the NSCA, the CNSC has a broad power to make regulations generally as it considers necessary for carrying out the purposes of the NSCA and to assist the CNSC in attaining its objects. Regulations are self-standing and legally binding and enforceable through enforcement measures embedded in the NSCA.

For the purposes of this report regulations may be divided into the following groups: 1) regulations of general application; 2) activity-specific and (or) facility-specific regulations.

Regulations of general application in nuclear security are the following:

1) *General Nuclear Safety and Control Regulations* establish general requirements for licence applications (further supplemented with additional requirements in other regulations), applications for licence to abandon, applications for renewal of licence, general obligations of licensees, obligations of workers, describe the concept of prescribed nuclear facilities, prescribed equipment and prescribed information. From the perspective of nuclear security area, the obligations of licensees (any person who is licensed to carry on an activity described in any of paragraphs 26(a) to (f) of the NSCA) include the obligation to maintain security of nuclear facilities and of nuclear substances (section 12(1.c), implement measures for alerting the licensee to the illegal use or removal of a nuclear substance, prescribed equipment or prescribed information, or the illegal use of a nuclear facility (section 12(1.g), implement measures for alerting the licensee to acts of sabotage or attempted sabotage anywhere at the site of the licensed activity (section 12(1.h)), instruct the workers on the physical security program at the site of the licensed activity and on their obligations under that program (section 12(1.j)). The Regulations also require licensees to report to the CNSC details related to actual or attempted security breaches or sabotage (section 29(1.e)) and issues related to safeguards equipment and samples (section 30(1.a–b)). Section 17(c.ii, c.iv) requires workers to inform the licensee of situations related to threats to nuclear security or sabotage, theft, loss or illegal use of a nuclear substance, prescribed equipment, or prescribed information;

2) *Radiation Protection Regulations* apply to those persons licensed to carry on an activity described in any of paragraphs 26(a) to (f) of the NSCA and set obligations of licensees and nuclear emergency orders such as to implement a radiation protection program, ascertainment and recording of doses, effective dose limits, etc. From the perspective of nuclear security area, the Regulations include general reporting requirements under section 16 in cases when licensee becomes aware that a dose of

radiation received by and committed to a person or an organ or tissue may have exceeded an applicable dose limit prescribed by the Regulations;

3) *Nuclear Security Regulations* apply to those persons licensed to carry on activities described in paragraphs 26(a), (b), (e), (f) of the NSCA (however, the applicability of specific requirements within the Regulations varies), i.e. the Regulations apply to all nuclear facilities and nuclear substances. The Regulations include clear definitions of the most important nuclear security concepts and establish requirements for nuclear security related information to be provided with the application for licence as well as nuclear security requirements to be met by the licensees (e.g., requirements concerning protected, inner and vital areas);

Nuclear Security Regulations (SOR/2000/209) Section15. (e) require that the SMR is manned all times by at least by one nuclear security officer. At the facilities visited by the IPPAS team, it was recognised that security relies heavily on detection of malicious acts in order to provide a timely security response. SMR is a crucial element for detection, because alarms are assessed there.

Suggestion: From the perspective of an insider adversary, the CNSC should consider amending the Nuclear Security Regulations in order to require at least two nuclear security officers to be present in the SMR for High Security facilities at all times; thus minimising the risk of an insider adversary.

In terms of assurances relating to fitness for duty at nuclear facilities and establishments, there is no regulatory requirement for sobriety tests for employees (or other persons) seeking access. The IPPAS team acknowledges the challenging legal path which any amendments to this situation may have to navigate in Canada and the ongoing CNSC-initiated engagement process intended to investigate Canadian jurisprudence boundaries in this area. Nonetheless, to provide security assurances which align broadly with other international partners, fitness for duty sobriety tests are very strongly encouraged.

Suggestion: On the basis of good international practice, drug and alcohol tests for persons entering the protected area. The CNSC should consider introducing a requirement to perform at least random drug and alcohol tests for persons entering the protected area to ensure they can safely carry out their daily duties.

4) *Packing and Transport of Nuclear Substances Regulations*, that apply in respect of the packaging and transport of nuclear substances (as described in the NSCA), including the design, production, use, inspection, maintenance and repair of packaging and packages and the preparation, consigning, handling, loading, carriage, storage during transport, receipt at final destination and unloading of packages, refer back to Nuclear Security Regulations for information to be provided with the application for licences to transport Category I, II and III nuclear material and licences to package or transport a nuclear substances (where the nuclear substance is Category I, II or III nuclear material).

5) *Nuclear Non-Proliferation Import and Export Control Regulations* provide regulatory controls on the import and export of controlled nuclear substances, equipment and information (includes a list of prescribed items) in order to ensure that Canada's nuclear non-proliferation policy and international obligations are respected.

Relevant activity-specific and (or) facility-specific regulations are the following:

1) *Class I Nuclear Facilities Regulations* apply to Class IA, which include, e.g., power reactors, and IB facilities, including, e.g. waste disposal facilities (classification is described in section 1). From the perspective of nuclear security area, the Regulations set information to be provided with applications for particular licences, e.g. in case of the licence to operate, – the obligation to provide information on

the proposed measures to prevent acts of sabotage or attempted sabotage at the nuclear facility, including measures to alert the licensee to such acts;

2) *Class II Nuclear Facilities and Prescribed Equipment Regulations* apply to Class II nuclear facilities, which are described as facilities that include Class II prescribed equipment (pursuant to section 1 of the Regulations that includes low-energy particle accelerators, irradiators, radiation therapy installations, etc.). In order to certify a model of Class II prescribed equipment, there is a clause with a general statement that the CNSC or the designated officer may request any other information that is necessary to enable the CNSC or the designated officer to determine whether the equipment model in question poses an unreasonable risk to the environment, the health and safety of persons or national security and whether certification of the equipment model would be in conformity with measures of control and international obligations to which Canada has agreed in the Regulations;

3) *Nuclear Substances and Radiation Devices Regulations* apply to all nuclear substances, sealed sources and radiation devices not covered by other regulations (all of the above and the Uranium Mines and Mills Regulations). Concerning security, the Regulations establish requirements such as, e.g.:

a) for an application for a licence in respect of a nuclear substance or a radiation device, other than a licence to service a radiation device, to contain information on the required by sections 3 or 4 (as applicable) of the *Nuclear Security Regulations* (where the application is in respect of Category I, II or III nuclear material, as defined in the *Nuclear Security Regulations*) (section 3(1.n.ii));

b) for every licensee who possesses or uses a nuclear substance or a radiation device and possesses, uses or produces an exposure device who becomes aware of e.g. the nuclear substance or the radiation device is lost or stolen, the exposure device or the sealed source assembly is lost, stolen or damaged to an extent that could impair its normal use to provide a report of the situation to the CNSC.

Pursuant to section 12(2) of the Regulations, in case of the application for certification of a model of a radiation device, the CNSC or the designated officer may request any other information that is necessary to enable the CNSC or the designated officer to determine whether the model of the device poses an unreasonable risk to the environment, the health and safety of persons or national security and whether certification of the model of the device would be in conformity with measures of control and international obligations to which Canada has agreed.

4) There are also *Uranium Mines and Mills Regulations* that apply to the uranium mines and mills, and subsection 3 (e) addresses requirements for nuclear security.

Emergency orders

Pursuant to section 47(1) of the NSCA, notwithstanding any other provision of the NSCA, in case of emergency the CNSC may, without conducting any proceedings, make any order that it considers necessary to protect the environment or the health and safety of persons or to maintain national security and compliance with Canada's international obligations.

Orders of the Governor in Council

The Governor in Council may, by order, issue to the Commission directives of general application on broad policy matters with respect to the objects of the Commission.

Licences and certificates

Pursuant to section 24(1) of the NSCA, the CNSC may establish classes of licences authorizing the licensee to undertake any activity described in any of paragraphs 26(a–f) that is specified in the licence for the period that is specified in the licence. Pursuant to section 24(5) of the NSCA, a licence may contain any term or condition that the CNSC considers necessary for the purposes of the NSCA. Accordingly, a licence typically includes information on the licensee, license period, licensed activities and the licence conditions, e.g. in the nuclear security area the licence condition is for the licensee to implement and maintain a nuclear security program.

In some cases, a licence is supplemented by a Licence Conditions Handbook, which is divided into sections reflecting safety and control areas (SCAs). Security is specified as one of the SCAs. The licence conditions handbook includes both mandatory standards which underpin regulatory expectations for compliance with the relevant licence condition and also refers to relevant compliance verification criteria. Within the Licence Conditions Handbook, requirements and recommendations are defined variously through the use of specific terminology. For example, "shall" or "must" are used to underpin the mandatory nature of the associated elements of the condition. Additionally, the Handbook also refers to recommendations and guidance, which afford opportunities to the licensee for interpretation of the most appropriate method of satisfying regulatory expectations.

The CNSC also issues certificates with respect to packages, special form radioactive material and low dispersible radioactive material.

III.2.3. Technical Guidance and other instruments

Regulatory documents

According to the information provided to the IPPAS team, the CNSC may issue regulatory documents, which provide guidance on how to comply with the established regulations or any other requirement. The scope of the regulatory documents is divided into 14 safety and control areas (SCA) and security is one of these 14 areas. Regulatory documents may refer to standards. The team noted extensive regulatory guidance provided to licensees on this issue.

Through "incorporation by reference" into the licence conditions the regulatory documents may be made obligatory to the licensees and the NSCA makes it obligatory to comply with any licence condition. It is an offence to fail to comply with any licence condition (NSCA, s. 48 (c)); power to impose any condition (NSCA, s.24 (5)).

According to the information provided to the IPPAS team, as an administrative tribunal created to regulate industry, the CNSC also has the administrative authority to issue guidelines and other non-binding instruments and this has been confirmed by the courts (e.g. *Ainsley Financial Corp. v. Ontario Securities Commission*, 1994, 21 O.R. (3d)104.

Standards

Standards (e.g. of the Canadian Standards Association) are used as references and through that may become mandatory documents, if referred to as such in the licence conditions and (or) the Licence Conditions Handbook. Standards could also be used as a reference in Acts and regulations and also become enforceable by this incorporation by reference.

Strategies and policies

The Canadian government approach to address significant matters is supported by strategies and policies. They are non-legally binding documents which broadly describe Government's policy, i.e. lays out how the Government intends to approach a relevant matter, e.g. "Securing an Open Society: Canada's National Security Policy", "Building Resilience Against Terrorism. Canada's counter-terrorism strategy".

The Acts, regulations and unclassified regulatory documents are publicly available. Acts and regulations are promulgated in the *Canada Gazette.* The regulatory documents are published in the CNSC's web site (this is done as a practice).

The provision of the NSS No. 13 para 3.2 for the physical protection regime to be reviewed and updated regularly from the perspective of legislation is implemented through implementing the CNSC's Regulatory Framework Plan. According to the information provided for the IPPAS team, the plan sets out the regulations and regulatory documents that are planned to be developed or amended. According to the plan, all published documents will be reviewed every five years. Pursuant to the Regulatory Framework Steering Committee Terms of Reference, the CNSC's Regulatory Framework Steering Committee is in charge of the Regulatory Framework Plan (developing, recommending for approval by Management Committee, monitoring and managing its implementation). This includes suggesting amendments to the plan if needed. The Regulatory Framework Steering Committee is also responsible for ensuring that CNSC's work with the CSA is aligned with the CNSC's regulatory framework priorities, ensuring that CSA's standards development and business plans incorporate a whole-of-CNSC perspective.

IV. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

Canada is a party to the Convention on Physical Protection of Nuclear Materials (CPPNM) and has ratified the 2005 Amendment to the CPPNM. Accordingly, it subscribes to the requirement of Fundamental Principle D: "The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities".

The IPPAS team was able to confirm that, to accord with such a requirement, responsibility and authority for the regulation of nuclear facilities and nuclear-related activities in Canada is assigned to the Canadian Nuclear Safety Commission (CNSC) by Parliament through the Nuclear Safety and Control Act (NSCA), which came into force in May 2000.

The NSCA created the Commission, set out its functions and powers, and set the framework for the regulation of the nuclear activity in Canada, assigning to the CNSC the authority to develop safety regulations, to make licensing and regulatory decisions and take enforcement action. Pursuant to section 10 of the NSCA, the Commission operates with up to seven permanent members (six part-time or full-time and one full-time member who acts as the President). Temporary members are appointed by the Governor in Council. Temporary members can be appointed as necessary. Newly appointed members swear an oath of fidelity, secrecy and submit themselves to a robust Canadian vetting security clearance process.

Pursuant to section 3 of the NSCA, the purpose of the Act is to provide for "the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks

to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information, and the implementation in Canada of measures to which Canada has agreed respecting international control of the development, production and use of nuclear energy including the non-proliferation of nuclear weapons and nuclear explosive devices".

Critically, in relation to security, one of the objects of the CNSC is to regulate, pursuant to subparagraph 9(a)(ii), the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information in order to prevent any unreasonable risk to national security associated with that development, production, possession or use.

The CNSC's status as the Competent Authority is not stated explicitly in legislation, although there is an assumption that the capabilities bestowed on the CNSC are sufficient to warrant its status.

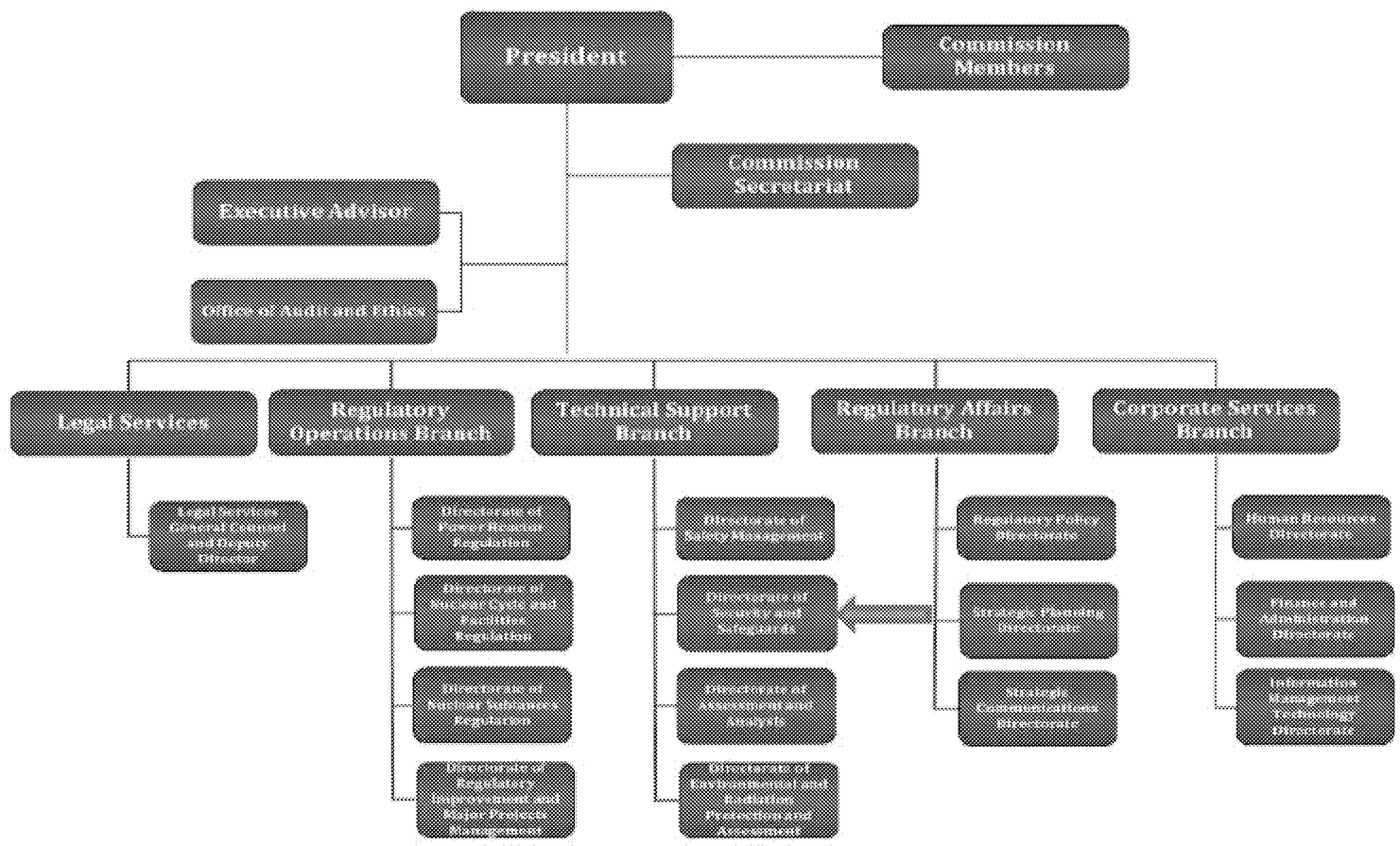

Figure 2. Canadian Nuclear Safety Commission Organizational Chart

The IPPAS team is satisfied that (by virtue of its quasi-judicial legal status, organizational structure, and the authorities vested in it under the NSCA), the CNSC demonstrates sufficient independence to satisfy the tenets of NSS No. 13, para 3.18.

IV.1. Licensing/Authorization Process

The CNSC has the authority to regulate all aspects of the nuclear industry in Canada through powers under the NSCA.

In terms of licensing, under section 26 of the Act, and subject to regulation, a licence from the CNSC is required in order for any qualified person to: possess, transfer, import, export, use or abandon a nuclear substance, prescribed equipment or prescribed information; to mine, produce, refine, convert, enrich, process, reprocess, package, transport, manage, store or dispose of a nuclear substance; produce or service prescribed equipment, operate a dosimetry service; or prepare a site for, construct, operate, modify, decommission or abandon a nuclear facility or construct, operate, decommission or abandon a nuclear powered vehicle or bring a nuclear-powered vehicle into Canada.

Additionally, under section 44 of the NSCA, the CNSC has the authority to make regulations respecting all matters of the regulation of nuclear substances and facilities in Canada.

Additionally, subsection 24(4) of the NSCA provides that no licence may be issued, renewed, amended or replaced and no authorization to transfer one given, unless such a process is authorized by the CNSC. The overall licensing process is shown in Figure 3.

NSS No. 13, para. 3.19 states that "The State's competent authority should have access to information from the State's system for nuclear material accounting and control."

The IPPAS team was able to confirm that, through the Nuclear Material Accounting System (NMAS), the CNSC was able to track inventories of materials at various licensee sites in Canada. Licensees are required to submit reports to CNSC regarding transfers and receipts of nuclear material. Data from these reports are entered into NMAS. In turn, reports are generated on a monthly and a quarterly basis and forwarded to the IAEA which is responsible for conducting monitoring and verification of nuclear material in Canada.

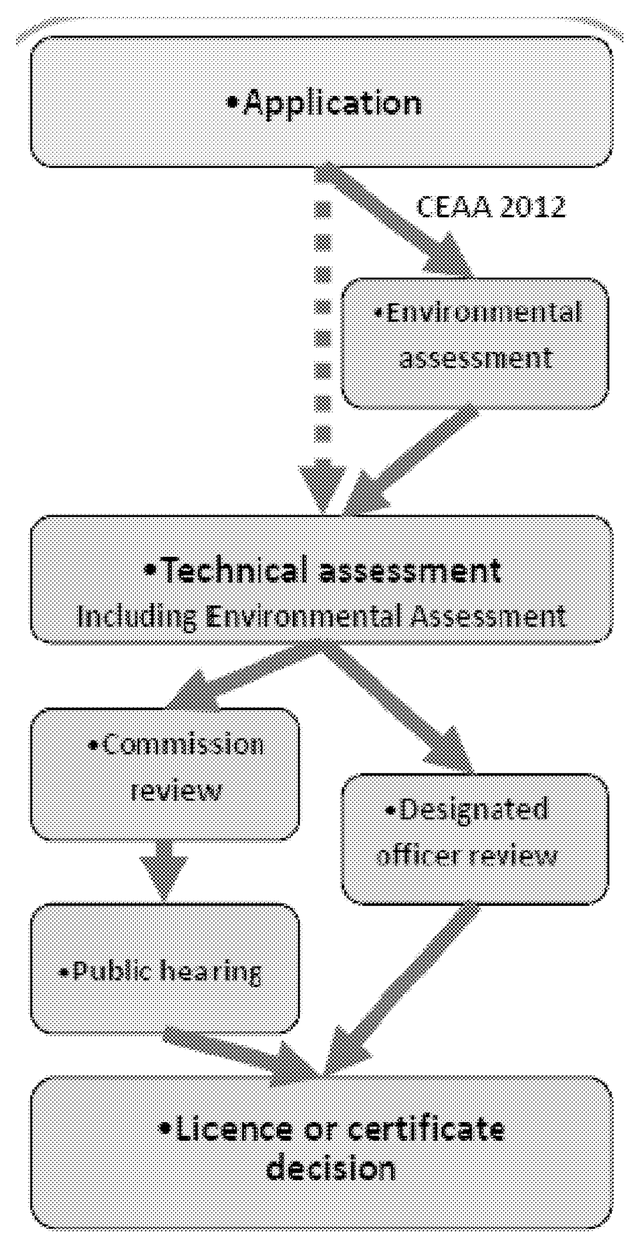

Figure 3. Licensing process

IV.2. Inspection and Enforcement

NSS No. 13, para. 3.20 requires that "The State's competent authority should be responsible for verifying continued compliance with the physical protection regulations and licence conditions through regular inspections and for ensuring that corrective action is taken, when needed."

The NSCA assigns to the CNSC responsibility for nuclear regulation and devolves powers to establish requirements, issues licences, and verify and enforce compliance. Accordingly, licensees must comply with the Nuclear Security Regulations under the NSCA, as well as other regulatory documents in the licensing basis.

Licensees must comply with the Nuclear Security Regulations under the NSCA, as well as with certain other provincial, territorial and municipal regulatory obligations. To assist with this process, the CNSC sets guidance and requirements to which the licensee must (in the case of requirements) or may (in the case of guidance) adhere.

A breach of the requirements may result in a variety of enforcement actions to include: an order, varying financial penalties or prosecution. The CNSC employs a variety of regulatory documents (REGDOCS) which supplement the compliance regime. These documents vary in classification, depending on the subject matter and afford licensees the opportunity to shape their own security regimes in order to meet regulatory expectations.

The CNSC was able to provide to the IPPAS team details of the powers and legal authority afforded to them under the NSCA. They hinge on sections 29 and 30 of the NSCA as the foundation of the regulatory inspection regime. These Sections assign various powers to inspectors as follows:

- subsection 29. (1) The Commission may designate as an inspector for the purposes of this Act any person whom the Commission considers qualified and any person so designated shall be provided with a certificate in the prescribed form certifying the person's designation.
- subsection 30. (1) In order to verify compliance with this Act, the regulations, an order or decision made under this Act or a condition of a licence, an inspector may, at any reasonable time and in accordance with the inspector's certificate, enter and inspect….

Physical security inspections are a key part of the CNSC's inspection program and the IPPAS team were satisfied that CNSC inspectors conduct planned (announced and unannounced) and reactive inspections in order to verify licensee compliance. Security inspections are conducted in accordance with CNSC approved processes. Considering the number of licensees and significant scope of the nuclear program, the IPPAS team deemed the CNSC security inspectorate insufficiently resourced.

Basis:
Amendment to CPPNM. Fundamental Principle D "Competent Authority. The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy."

NSS No. 14 para 3.7 "The State should ensure that the regulatory body and other competent authorities are adequately provided with the necessary authority, competence and financial and human resources to fulfil their assigned nuclear security responsibilities".

NSS No. 14 para 3.29 "The State should commit the necessary resources, including human and financial resources, to ensure that its nuclear security regime is sustained and effective in the long term to provide adequate nuclear security for radioactive material".

Recommendation: Taking into account the scale of the Canadian civil nuclear and radiological programme and the wide geographic distribution of regulated entities, the CNSC should review the current security programme to determine the adequacy of resources underpinning its regulatory remit.

Pursuant to subsection 8(2) of the NSCA, the CNSC may exercise its powers only as an agent of Her Majesty. Nonetheless, the IPPAS team was informed that the CNSC believes its present status does not undermine the principle of independence. Indeed, the CNSC states it demonstrates sufficient independence to fulfil this requirement through its authority and power to employ the staff required to meet its mandate. Section 16 of the NSCA gives the CNSC authority to appoint and employ the professional, scientific, technical and other staff it considers necessary to carry out its responsibilities. The CNSC also sets its own classification scheme and, in consultation with the Canadian Treasury Board, sets salary levels. Additionally, the competence of the CNSC inspectorate is confirmed through a corporate governance and assurance process which requires all personnel to undertake appropriate training and validation of individual skills and abilities.

IPPAS was also informed that the CNSC's status as a separate employer contributes to its independence and allows a rapid response to changes in the labour force. Additionally, the IPPAS team was informed that the CNSC operates a new funding regime whereby it receives funding from two sources in order to discharge its mandate. Those sources are, the CNSC believes, sufficient to ensure independence and come from 25% Parliamentary Appropriation (where the CNSC, through the Treasury Board of Canada, receives an authority from Parliament to expend resources from Canada's treasury), and 75% fees paid by applicants, licensees and other special project sponsors in accordance with the CNSC Revenue Spending Authority. Accordingly, the Commission has the statutory authority to prescribe and charge fees for the services and products it provides under the NSCA.

In terms of its independent authority, the CNSC is authorised, pursuant to section 47 of the NSCA, to issue emergency orders without conducting any proceedings. Importantly such orders may be issued pursuant to subsection 47(1), when CNSC considers it necessary to protect the environment or the health and safety for persons or to maintain national security and compliance with Canada's international obligations.

Finally, CNSC commissioners are subject to post employment rules. These obligations are also enforced while they are employed by the Government of Canada as well as for a period of one year following the termination of their employment.

IV.3. Coordination with other State Organizations That Contribute to Nuclear Security

The CNSC, in its capacity as Competent Authority for regulation of nuclear and radiological nuclear materials and as an Agency of the federal government, engages with a number of other Canadian organisations which contribute to nuclear security.

Specifically, in terms of emergency preparedness, the CNSC contributes to Public Safety and Emergency Preparedness plans at Federal, Provincial and local levels. The organisations with which CNSC engages includes (but is not limited to), Public Safety Canada, which takes the lead in this area. Additionally, through its contribution to the Federal Emergency Response Plan (FERP) and more specifically, the Federal Nuclear Emergency Plan (FNEP), CNSC is a critical enabler to the development of a multi-agency nuclear 'rich picture' which informs national understanding on nuclear and radiological issues. In Canada, the CNSC also engages closely with a host of other national departments and agencies involved specifically in intelligence analysis and security policy. They include (but are not limited to), the CSIS, the RCMP and the Canadian Integrated Threat Assessment Centre (ITAC).

Finally the IPPAS team noted and applauds a firm commitment in Canada and on the part of the CNSC to the principle (where appropriate) of transparency in delivery of its outputs.

IV.4. International Cooperation and Assistance

Canada is one of the largest contributors to the IAEA Nuclear Security Fund. Canada is also actively participating in many security related international initiatives including funding for the Global Partnership Program (GPP) - to enhance nuclear and radiological security.

In addition to what was mentioned in the section II.1.2 (Executive branch) on the network of the international and multilateral cooperation, it should be noted that Canada provides its security experts to IAEA IPPAS and other missions.

V. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)

As part of the construction of a fully functional national protective security regime, states which subscribe to the principles of the Convention on the Physical Protection of Nuclear Materials (CPPNM) and consequently the security elements of IAEA NSS No. 13, must create an analytical process against which physical protection systems at civil nuclear facilities and licensees should be developed, measured and tested.

Accordingly, to satisfy CPPNM Fundamental Principle G, “The State’s physical protection should be based on the State’s current evaluation of the threat”. Additionally, to ensure any Threat Assessment is comprehensive and relevant, NSS No. 13, para. 3.35 requires that “States should ensure the Competent Authority has access to information from other organisations in the State on present and foreseeable threats to nuclear activities.”

In Canada, the Threat Assessment incorporates classified, all-source intelligence from Government stakeholders engaged in intelligence and security. Those stakeholders include (principally, but not exclusively), the CSIS, the RCMP and the ITAC. Additionally, the IPPAS team received assurances that contributions to the Threat Assessment, utilizing sensitive intelligence, are garnered from a variety of valuable international strategic security partnerships to which Canada subscribes.

Good Practice: The CNSC’s maintenance of a dedicated threat intelligence section ensures that the Canadian civil nuclear industry benefits from a mature, well-balanced and comprehensive national intelligence framework, supported by national and international security and intelligence partnerships. In Canada, the process of development for the Threat Assessment utilizes the standard Intelligence Cycle, incorporating the following four phases: Direction, Collection, Analysis and Dissemination. The IPPAS team confirmed that the CNSC is embedded in this process.

Once the Threat Assessment is complete, NSS No. 13 requires that “The State’s physical protection requirements for nuclear material and nuclear facilities should be based on a design basis threat, specifically for …”, unauthorized removal of Category I nuclear material and the sabotage of nuclear material and nuclear facilities which have potentially high radiological consequences.

The IPPAS team received assurances that such a requirement is enshrined within the Canadian Nuclear Security Regulations (NSR) which confirms that “The Commission shall establish a design basis threat analysis and update it as necessary...” and within the CNSC the responsibility for delivery of the design basis threat falls directly to the Nuclear Security Division (NSD) of the CNSC.

The IPPAS team were able to confirm that the CNSC NSD were competent, capable and well connected, both through robust intelligence liaison relationships and by virtue of the security clearance levels of their personnel. Possession of such clearances affords access to the most sensitive levels of the Canadian Government intelligence infrastructure.

The IPPAS team received assurances that the Canadian Design Basis Threat applies to high security sites in Canada: specifically nuclear power plants or nuclear facilities where Category I or II materials are processed, used or stored. Additionally, the IPPAS team was assured that the Canadian Design Basis Threat contains clear, unambiguous statements relating to the motivations, intentions and capabilities of potential adversaries. Finally, the IPPAS team received assurances that the document was similarly applicable to those licensees which transport such materials.

NSS No. 13, para. 3.37 also states that "The State should decide whether to use a threat assessment or design basis threat for other nuclear material and nuclear facilities."
In this regard, the IPPAS team was able to confirm that, for Category III material and facilities and security of radioactive material and associated facilities, a threat assessment is the sole basis for the basis of protection requirements.

The legally-mandated ever-changing nature of the design basis threat (aimed at ensuring levels of currency) allowed the CNSC to confirm to the IPPAS team its ongoing international engagements relating to the development of a 'Cyber DBT'. Specifically, the CNSC confirmed they were contributing to the IAEA-sponsored forum on this issue. The IPPAS team was also able to confirm that the CNSC anticipate such a revised version of the Design Basis Threat would include references to a variety of threat vectors (insider, external attacker and a 'blended' attack whereby a physical attack is accompanied by a cyber one).

At the conclusion of the drafting process, the CNSC Design Basis Threat is classified CANADIAN EYES ONLY SECRET and protected accordingly – both within the CNSC and by those licensees authorized to receive it.

NSS No. 13, para. 3.40 states that "The State should give attention to providing protection measures against any airborne threat and against possible stand-off attacks specified in the State's threat assessment or design basis threat."

In addition, the IPPAS team was able to confirm that the Canadian document also considers both airborne threat and stand-off attacks. Airborne threat is considered Beyond DBT and therefore beyond the responsibility of the licensee. Accordingly, it is mitigated through the various controls (legal, regulatory and administrative), at the local, regional, provincial and national levels. In this regard, Public Safety Canada (PS) has the national lead and is able to activate the National Air Incident Protocol, which may require Canadian military assistance.

NSS No. 13, para. 3.39 states that "The State should continuously review the threat and evaluate the implications of any changes in the threat assessment or design basis threat."

The Canadian Design Basis Threat does not have a mandated, fixed timetable for review. Rather, the IPPAS team were advised, threats are monitored on a daily basis and tested against the very latest intelligence (to which the NSD has access). Notwithstanding this lack of a defined timetable for review, the Design Basis Threat is currently undergoing such a process.

Suggestion: The CNSC should consider introducing a defined timetable for review of the Design Basis Threat, which may deliver a helpful rhythm to the process of updating the document.

The IPPAS team was able to confirm, through its visit to Bruce Power, that the Design Basis Threat is the foundation upon which licensees frame their physical protection capabilities and base associated vulnerability assessments. Additionally, at the tactical level, the document is also used as a basis for the development of adversary scenarios against which licensees and the CNSC undertake performance testing.

Whilst at Bruce Power, the IPPAS team confirmed the adversary scenarios used in performance testing stem from an analysis of the motivations, intentions and capabilities of an adversary as described in the Design Basis Threat. Accordingly, the CNSC has created the Canadian Adversary Testing Team (CATT). The CATT consists of a cadre of specially selected Nuclear Response Force personnel drawn from across the civil nuclear estate who undertake the role of adversaries during site performance testing. The existence of this capability ensures that there is a clear understanding on the part of licensees of the most likely TTPs of any adversary and this delivers a clear line of logic from strategic to tactical level.

Good Practice: The development, maintenance and utilization of a specific "Adversary force" such as the CATT allows a clear line of understanding amongst licensees of the most likely and most dangerous TTPs of any potential adversary. Such knowledge ensures that training and exercising against Design Basis Threats employ both currency and realism.

To add to the comprehensive nature of the Design Basis Threat, the IPPAS team was able to confirm that many licensees operate a complementary tactical area of intelligence responsibility, endorsed and encouraged by the Regulator.

Additionally, (in accordance with Section 7.5 (1) of the NSRs), licensees undertake (at least once every twelve months) a Threat and Risk Assessment specific to their facilities, in order to determine the adequacy of their physical protection systems. The Threat and Risk Assessment identifies the facility assets which require protection from sabotage and unauthorized removal. After determining these assets, the vulnerabilities and the threats to the assets are examined.

Good Practice: The regulatory requirement for a licensee to deliver an annual tactical Threat and Risk Assessment.

Finally, although changes to national threat levels are unclassified and disseminated widely throughout Canada, the IPPAS team was able to confirm that the CNSC's involvement at the heart of the Canadian national security infrastructure allows it privileged access to the sensitive reporting relating to emergent threats. In most cases, licensees who possess the appropriate physical protection systems at their facilities can be provided with classified information by the CNSC Nuclear Security Intelligence Section utilizing accredited secure voice and fax capabilities. In the case of such specific (sensitive) reports, the CSNC - with the approval of the originator – is able to disseminate classified information to licensees.

Good Practice: The utilization of classified technology (e.g. secure phone, fax), accessible to suitably cleared licensees complements the rapid and comprehensive dissemination of security updates.

The IPPAS team considers that the CNSC complies with the tenets of Fundamental Principle G.

VI. RISK INFORMED APPROACH

The CNSC has adopted a risk informed approach in the regulation of all facilities and activities to ensure the allocation of resources and level of reviews, assessments and inspections commensurate with the overall risk of the facility and activity, implementing key security principles of graded approach and defence-in-depth.

VI.1. Risk Management

The risk informed approach used in Canada is based on a process derived from the Canadian Standards Association (CAN/CSA-Q850-97), "Risk Management: Guideline for Decision-Makers." The purpose of the guideline is to provide a comprehensive decision making process that will aid decision makers in identifying, analysing, evaluating, and controlling all types of risks, including risks to health and safety. The guideline notes the objective of risk management is to ensure that significant risks are identified and that appropriate action is taken to minimize the risks as much as is reasonably achievable.

CNSC Regulatory Policy, "Regulatory Fundamentals, P-299," Section 4.4. "Basic Regulatory Action on Level of Risk" states that the CNSC: 1) regulates persons, organizations, and activities that are subject to the act and regulations in a manner that is consistent with the risk posed by the regulated activity; 2) recognizes that risk must be considered in the context of the CNSC's mandate under the Act; and 3) makes regulatory decisions and allocates resources in a risk informed manner.

VI.2. Graded Approach

CNSC Nuclear Security Regulation (SOR/200-209) is consistent with the fundamental principle of graded approach in that it takes into account the current evaluation of the threat, the relative attractiveness, nature of material and potential consequences of its unauthorized removal and sabotage against nuclear facilities or nuclear material. NSR section 7.4(2) states that the Commission shall provide the current design basis threat to every high security site licensee, who shall take that analysis into account in the design of their physical protection system and make modifications to that system as necessary. Furthermore, section 7.5(2) states that every licensee shall make modifications to its physical protection system, as necessary, to counter any credible threat identified as a result of the threat and risk assessment. In order to determine the appropriate levels of protection are provided, the regulations define "high-security site" as a nuclear power plant or a nuclear facility where Category I and II nuclear material is processed, used or stored.

The material categorization table in the NSR for Categories I, II and III nuclear material follows the Amendment to the CPPNM and NSS No. 13 with the exception of the established specific requirements for plutonium in irradiated fuel. Unlike the Amendment to the CPPNM and NSS No. 13 which does not specifically mention plutonium in irradiated fuel, the NSR identifies more than 500 grams of plutonium as Category II material and 500 grams or less, but more than 15 grams of plutonium as Category III.

The NSR categorization table also provides clear guidance on aggregation of material. A footnote for Category I-III states, "The quantities listed refer to the aggregate of each kind of nuclear substance located at a facility, excluding the following (which are considered separate quantities): (a) any quantity of the nuclear substance that is not within 1,000 meters m of another quantity of the nuclear substance; and (b) any quantity of the nuclear substance that is located in a locked building or a structure offering similar resistance to unauthorized entry."

VI.3. Defence in Depth

The CNSC's regulatory approach is consistent with the fundamental principle of defence-in-depth in that it requires several layers and methods of protection (structural or other technical, personnel, and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives. The CNSC uses both prescriptive and performance based regulations due to the

complexities of the facilities and activities being regulated. The NSR are based on the concept of defence-in-depth principle which includes detection, delay and response. The regulations include requirements for: protected, inner and vital areas; intrusion detection; off-site response force; access control, security clearance, verification of identity.

VII. SUSTAINING THE PHYSICAL PROTECTION REGIME

VII.1. Security Culture

Nuclear security culture is led from the highest Government levels as demonstrated through Canada's efforts domestically and internationally to ensure the safe and secure use, storage and transportation of nuclear and other radioactive materials and facilities. The CNSC as a Governmental, independent authority applies same principles than other Governmental bodies for security culture.

The Prime Minister (PM) released a written national statement at the Nuclear Security Summit (NSS) and delivered a summary of the statement in plenary. The statement addresses Canada's fulfillment of its past NSS commitments and on new Canadian initiatives. This refers Canada's strong support for the NSS and ongoing prioritization of nuclear security at the domestic and international level.

The IPPAS team considers Canada to have strong elements of security culture but currently there is no document to demonstrate the national commitment to provide guidelines to the organizations and to set out the organization's security culture similar to the safety culture. The CNSC informed the IPPAS team that security culture is embedded within the safety culture at CNSC. At the facility level, nuclear security is prevalent in all aspects of the operations

In principle, safety and security cultures coexist and need to reinforce each other because they share the common objective of limiting risk. There will be occasions where there are differences between safety and security requirements. Therefore, an organization in charge of nuclear matters has to foster an approach that integrates safety and security in a mutually supporting manner. It was recognized by the IPPAS team that there is a strong commitment to the safety culture in the CNSC and the elements of security culture exist as well. At the moment there are no documents which specifically refer to nuclear security culture. However, notwithstanding NSD (Nuclear Security Division) involvement in the drafting process of REGDOC-2.1.2, Management System Safety Culture, the IPPAS team did not identify any reference to nuclear security culture in the draft document.

Suggestion: The CNSC should consider using the development of its Management System Safety Culture document as an opportunity to explicitly refer to nuclear security culture and its importance. Useful guidance can be found in IAEA NSS No. 7.

The CNSC appointed a dedicated security awareness officer. His/her duties/responsibilities are in summary: develop and deliver a commission wide-security and safety awareness program, develop, review, revise and monitor Security policies and follow the establishment and implementation of a security awareness communication and training program. The IPPAS team considers this as a good practice.

Good practice: The CNSC has appointed a dedicated security awareness officer with responsibilities for the security awareness program within the CNSC.

VII.2. Quality Assurance

The CNSC requires that, in order to appropriately protect the public and the environment, licensees establish, implement, assess and continually improve a management system in which safety is the highest priority. The elements of the system are normally integrated. The CNSC oversight review of the licensee management system is completed during the licensing stage and is verified at each licence renewal.

The CNSC Management System is a system managed by CNSC and it is informed by IAEA GS-R-3 Standard (nuclear regulatory excellence) and Treasury Board Secretariat's Management Accountability (excellence in management). Elements of the CNSC Management System are shown in Figure 4.

Since 2009, the CNSC has required that licensees have a Management System for the licensed activity that extends to all safety and control areas, The management system standard, CSA N286, has safety as the primary deliverable. The management system describes all policies, plans and processes on how the licensee has to meet requirements.

The CNSC specifies that a licensee's management system shall apply to all safety and control areas. N286-05 supports this further by having security as a specific requirement to which all generic elements apply. N286-12 integrates the management system requirements for health, safety, environment, security, economics and quality, which is of paramount importance in all decisions and actions once a licence has been issued. The CNSC verifies the performance of the management system, and especially the performance of the licensee in delivering its key processes/programs. REGDOC 3.1.1 Reporting Requirements for Nuclear Power Plants requires quarterly reporting and program reporting.

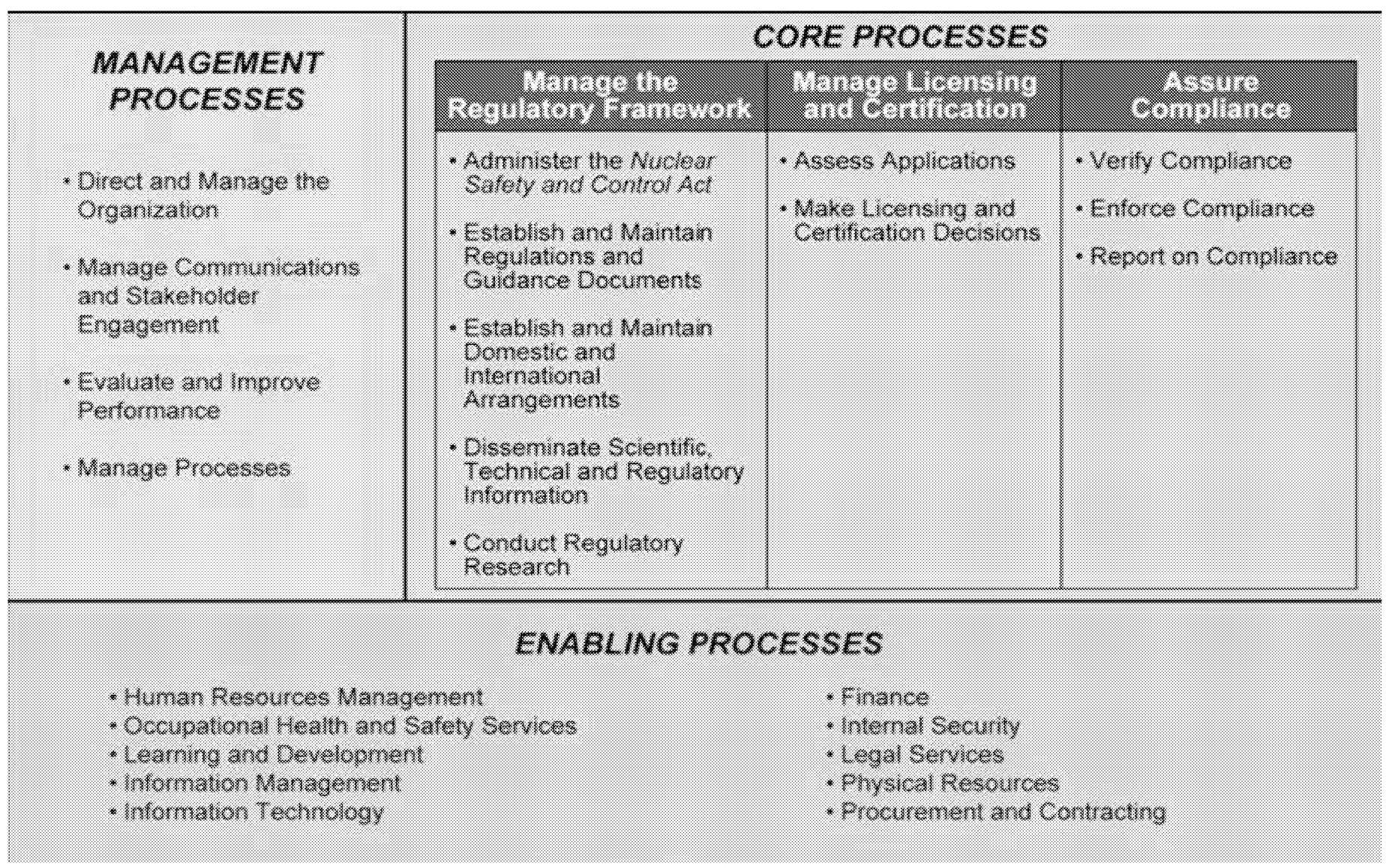

Figure 4. Management System Processes

Class I Regulations, the *Class II Regulations* and the *Uranium Mines and Mills Regulations* require information to be submitted on "the … quality assurance program for the activity to be licensed". The

Class I and Class II Regulations also require information to be submitted on "the proposed measures, policies, methods and procedures for operating and maintaining the nuclear facility". Quality assurance requirements are also imposed through licence conditions; for example, power reactor operating licences generally require that the licensee meet the requirements of CSA/N-286 on quality assurance. CNSC staff verifies that safety is being managed adequately by means of the compliance program, which describes regulatory oversight activities of promotion, verification and enforcement.

VII.3. Confidentiality

In Canada, limiting access to classified information is achieved through various acts and legislation including adherence to Treasury Board guidelines for protecting information and applying appropriate clearances. (Policy on Government Security, 2009 Treasury Board of Canada Secretariat and through GNSCR sections 21 to 23 and Nuclear Security Regulations.) CNSC also uses the term "prescribed information" in regard to the protection of sensitive information dedicated to security. Prescribed information is defined under the General Nuclear Safety and Control Regulations. Further, for those organizations or licensees who may not be subject to Treasury Board guidelines for protecting information and applying appropriate clearances (Policy on Government Security, 2009 Treasury Board of Canada Secretariat) protection requirements of "equivalencies" are required (see REGDOC-2.12.2 *Site Access Security Clearance*).

Nuclear Security Regulations requires protection of information and trustworthiness verification. Guidance at the federal level is applied in accordance with Treasury Board Guidelines and at the facility level in accordance with requirements for clearances in the NSR section 18(3), 18.1 and 18.2.

The IPPAS team was informed that all information under the custodianship of the CNSC requires an appropriate level of protection. Information and assets must be protected and the sensitivity of information is determined based on the degree of injury that would result from its unauthorized disclosure, destruction, removal, modification, interruption or use. Figure 5 shows how the classification of sensitive information is done based on degree of injury. The Government of Canada security policy divides information other than that which is considered "non-sensitive" or "publicly available" into two categories: Classified and Protected.

	Classified	Protected
Low injury	Confidential	Protected A
Medium injury	Secret	Protected B
High injury	Top Secret	Protected C

Figure 5. Classification of Sensitive Information

CNSC also applies the "need-to-know" principle to classified information. Staff and management are not entitled to access information merely because of their status, rank or office, they must request access only to the information for which they have an absolute need in order to perform their duties.

The "Need to Know" principle is established by determining whether or not the operational or administrative objective could be achieved without access to the sensitive information in question.

The IPPAS team was advised that the storage of physical documents is stored in containers appropriate to their sensitivities:

- Protected A – stored out of plain sight
- Protected B – in operations zone, stored in a security container
- Protected C and Confidential – in operations or security zone, stored in a safe or security container
- Secret – in a security zone only, stored in a safe or security container
- Top Secret – in a security zone only, stored in a safe

Additionally, the IPPAS team was informed that there are detailed requirements on how to transmit, destroy and handle classified documents. Details of these requirements are confidential. Electronic documents of business value are stored in the CNSC corporate repository "e-Access" and sensitive electronic documents are stored either on non-networked encrypted laptops or on Iron Key USB keys, those are treated like sensitive physical documents.

The CNSC email-system can be used to send electronic documents up to and including Protected A designation. In the Government of Canada, my Key solution is leveraged to encrypt sensitive documents. A Managed Secure File Transfer connection may be set up for a specific licensee who has to share sensitive documents frequently with the CNSC. With the certain exceptions, encrypted Iron Key USB keys are used to transport electronic documents.

A variety of awareness and training tools are provided at the CNSC. Employees must complete mandatory online security training and managers an in-class Management Fundamentals course.

VII.4. Sustainability Programme

The IPPAS team was informed that at the national level a number of sustainability principles are applied:

- National commitment
- Legislative & regulatory framework
- Roles, responsibilities and accountability
- National threat assessment
- Planning & organization
- Developing human resources
- Fostering a nuclear security culture
- Oversight of the regime

National commitment is based on threat recognition and international obligations for safety and security and ensured through national nuclear security policy, threat assessment, and adaptive security policy reviews.

NSR sections 30 and 37(2) require that duties have to be defined and that procedures must exist to support them. Staffing, particularly at high security facilities, is monitored through various means including reporting on staff complement and minimum staff complements to meet and counter the threats to facilities. NSR section 30 requires a sufficient number of nuclear security officers.

The CNSC monitors the licensee programs for equipment maintenance and lifecycle management of systems and devices. Further to the monitoring and reporting requirements of the operator, testing of devices is also required to be undertaken where applicable by the operators. Criteria, where appropriate, is provided.

The management system standard CSA N286 is the licensing basis for NPPs and it requires a licensee to plan their business, identify resources required and set up an organization. Staffing at high security facilities is monitored through various means including reporting on staff complement and minimum staff complements to meet and counter the threats to facilities.

Review of procedures and maintenance of programs are undertaken by licensees, and these activities and documents are reviewed by the CNSC.

For example:

- RD-321 *Criteria for Physical Protection Systems and Devices at High-Security Sites*

- RD-361 *Criteria for Explosive Substance Detection, X-ray Imaging, and Metal Detection Devices at High-Security Sites*
- Other general requirements also exist for maintenance, repair, and calibration.
- For example, the following regulatory documents are part of the licensing bases for existing NPPs.
- RD/GD-210 *Maintenance Programs for Nuclear Power Plants*
- RD/GD-98 *Reliability Programs for Nuclear Power Plants*
- *REGDOC 3.1.1.Reporting Requirements for Nuclear Power Plants*

Nuclear Power Plants have requirements to report in case the Physical Protection System is not operating as planned. Licensees conduct performance testing and operational monitoring of their processes, systems and devices. Performance testing and operational monitoring are undertaken by the regulator through inspection and surveillance activities, exercises and reporting by the operators.

Configuration and change management processes are required to be in place through the management system(s) of the operators.

The license basis includes CSA N286 standard which has a requirement for controlling changes. Also, for configuration management, the standard language on document and records control and training are directly applicable. The specific requirements for design changes, etc., for components are included in the standard as well as in other CNSC documents.

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

As part of CPPNM, Fundamental Principle K: Contingency Plans, there is a requirement for the development and maintenance of contingency (emergency) plans to respond to unauthorized attempts to remove nuclear material or sabotage of nuclear facilities or nuclear material. Additionally, INFCIRC/225/Rev5, Para 3.58 states that "The State should establish a contingency plan. The State's competent authority should ensure that the operator prepares contingency plans…".

The IPPAS team was able to confirm that, in the case of Canada, the safety of Canadian citizens is a Government of Canada priority. Accordingly, Public Safety Canada coordinates departments and maintains overall responsibility for national security.

The Minister of Public Safety and Emergency Preparedness, in consultation with the Minister of Foreign Affairs, is responsible for the implementation of Canada's Counter-Terrorism Strategy . The strategy assesses the nature and scale of the threat and sets out basic principles and elements which underpin the Government's counter-terrorism activities. According to Section 3 of the Emergency Management Act, the Minister of Public Safety is responsible for exercising leadership relating to emergency management in Canada by coordinating, among government institutions and in cooperation with the provinces and other entities, emergency management activities. The Minister has a wide variety of tasks, including: provision of advice to government institutions with respect to the preparation, maintenance, testing and implementation of emergency management plans; analysing and evaluating emergency management plans prepared by government institutions; and coordinating the Government of Canada's response to an emergency.

Public Safety Canada was created in 2003 to ensure coordination across all federal departments and agencies responsible for national security to protect Canadians and their communities, businesses and interests from a range of risks such as natural disasters, crime and terrorism. Public Safety Canada functions as a centralised hub for coordinating work in counter-terrorism, critical infrastructure and computer security. Public Safety Canada engages Canadian citizens to ensure it fulfills its mandate

and is also responsible for developing policies and providing advice to the Minister of Public Safety and Emergency Preparedness.

Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) are addressed in a similar manner to other national disasters. Accordingly, responses take place at local, Provincial and Federal levels. The IPPAS team was informed that the key elements underpinning these national emergency plans focus on the classic four components of emergency preparedness: Prevention, Preparedness, Response & Recovery and deliver a Federal Emergency Response Plan (FERP).
Within the FERP, there is also a Federal Nuclear Emergency Plan (FNEP). This enshrines the nature of any governmental emergency response and intervention capability for a major nuclear emergency. It is a multi-departmental, event-specific plan which outlines the roles and responsibilities for federal organisations in preparing for and responding to nuclear emergencies.

At the regulatory level, the *Nuclear Security Regulations* (NSRs), which are largely based on INFCIRC/225/Rev 5, direct the licensee to develop strategies to prevent theft and sabotage and this extends to a requirement (under Section 36 of the NSRs) to develop contingency plans in conjunction with off-site response forces for an "effective intervention" based on the Design Basis Threat. The IPPAS team was able to confirm that REGDOC 2.12.1 (High Security Sites: Nuclear Response Force), which was developed in conjunction with a variety of federal, provincial and local law enforcement agencies, sets out the Regulator's expectations in this regard.

The details within the document include specifications for: the composition of a Nuclear Response Force (NRF); the nature of mandatory assets and firearms and associated authorisations under which the force should operate; standards and criteria for selection of NRF personnel; the nature of training and testing for NRF personnel; the nature of NRF vehicles, command posts and equipment; standards to be employed for the maintenance and storage of special equipment operated and utilized by the NRF; the nature of tactical deployment of the NRF; off-site Response Force arrangements; the requirement to report security events.

In the case of reporting nuclear security events, the licensee is required to report the occurrence of specific security incidents to the CNSC in accordance with a specific timetable which specifies the relative immediacy of the reporting requirement and sets out the need for the licensee to deliver a full report on the matter to the CNSC within twenty-one days after becoming aware of the event. The list of events to be reported include, amongst other things, any attempted or actual breach of security or any attempted or actual act of sabotage at the licensed site.

In terms of the requirement to prepare for the recovery of nuclear materials following any incident, the REGDOC 2.10.1 specifies that all licensees shall maintain plans and procedures which allows for the process to transition from emergency response to recovery after the termination of an emergency, including the requirements to establish a recovery organization and to develop a recovery plan. Additionally, the REGDOC requires that licensees shall identify, in the recovery plan, the positions/titles, authorities and responsibilities of the individuals who will fill key positions in the recovery organisation; this organisation shall also include technical personnel with responsibilities to develop, evaluate and direct recovery and re-entry operations.

NUCLEAR FACILITY REVIEW (MODULE 2)

Canada operates a very large peaceful nuclear programme, which includes almost all elements of the fuel cycle, including uranium mining and milling, refining, nuclear fuel fabrication, nuclear power, research reactors and waste management facilities.

Canada is the world's second-largest uranium producer and 85% of Canada's uranium production is exported.

Nuclear power plants in Canada are located at five sites in three provinces and are operated by four separate licensees. There are nineteen reactors units operational at Darlington, Pickering, Bruce Power and Point Lepreau. Pickering Units 2 and 3 remain in safe storage and Gentily-2 has transitioned to safe storage. All power reactors are of the CANDU (CANada Deuterium-Uranium) design originally developed by the Canadian Crown Corporation Atomic Energy of Canada Limited (AECL), NPPs produce about fifteen percent of Canada's electricity.

There are six operating research reactors situated at sites: Chalk River Laboratories, McMaster University, École Polytechnique, Saskatchewan Research Council, University of Alberta and Royal Military College of Canada.

There are also several Used Fuel Dry Storage Facilities in operation in Canada. Three nuclear facilities were visited and security measures in place reviewed by IPPAS team during the mission. The results of the facility review are provided in the next three chapters of the report.

IX. BRUCE NUCLEAR GENERATING STATION

Formed in 2001, Bruce Power is Canada's first and only private sector nuclear generator and operates the largest nuclear power plant in the world, producing 6,300 MW (Bruce A and B combined), or over 30% of Ontario's electricity. Bruce Power has eight operating CANDU® (Canadian Deuterium Uranium) reactors (the Bruce A and B generating stations each hold four reactors) at the company's site in Tiverton. In addition to Bruce A and B generating stations, the Douglas Point Waste Management Facility and Western Waste Management Facility are also situated at the Bruce Power site (see the figures 6 & 7 below).

Bruce Power's 2,300-acre site is situated on the shores of Lake Huron, between the towns of Kincardine and Saugeen Shores, 250 km northwest of Toronto. The site is leased from the Province of Ontario under a long-term arrangement where all of the assets remain publicly owned; while the company makes annual rent payments and funds the cost of waste management and eventual decommissioning of the facilities. Due to geographic isolation, the Bruce Power site is, for all intents and purposes, a self-sufficient community.

Bruce Power currently employs over 4100 people in various departments, and employs up to an additional 4000 contractors. A majority of Bruce Power's employees are also owners in the business.

As part of the mission programme, the IPPAS team visited Bruce B generating station (see figures No. 6 and 7 below) and was able to observe practical implementation of security measures at this facility as well as to discuss security related issues with the security management and security personnel.

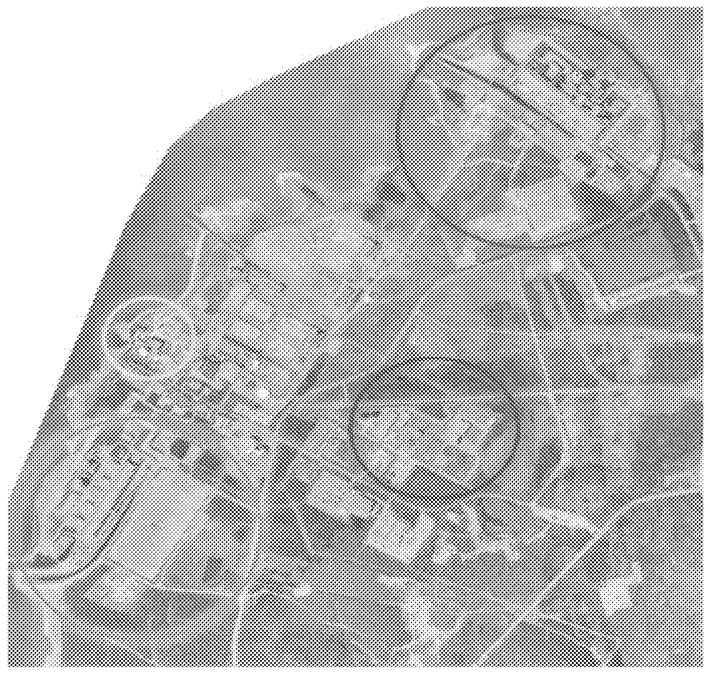

Figure 6. Bruce Nuclear Site

Figure 7. Bruce Nuclear Generating Station

IX.1 Security Management Programme

The Nuclear Security Program operated by Bruce Power includes: threat and target identification, structure and elements of the security organization; interfaces with nuclear material accountancy and control and nuclear safety; reporting of nuclear security events; system evaluation and performance testing; physical, technical and administrative protection measures to support access control and response; security clearance; investigative/intelligence services; threat risk analysis and implementation of security countermeasures to mitigate risk. The program ensures sustainability and continuous improvement using the Plan-Do-Check-Act model.

IX.1.1.Threat and Target Identification

The CNSC delivers the Design Basis Threat to the facility operator. According to the Nuclear Security Regulations (SOR/2000/209) Section 7.4 (2) The Commission shall provide a current design basis threat analysis to every licensee, who shall take that analysis into account in the design of physical protection system. Section 7.5 (1) requires every licensee to conduct a threat and risk assessment (TRA) specific to that facility at least every twelve months. It is also required by the CNSC that modifications shall be undertaken by the operator in respect to the TRA.

The Nuclear Security Regulations (SOR/2000/209) Section 14.1 requires the licensee to identify all vital areas taking into account design basis threat and other relevant information. During the visit, the IPPAS team was provided basic information on how the licensee satisfies these requirements. Vital area identification is undertaken utilizing CARVER methodology and the measures to protect the vital areas (as required by the CNSC) are defined. Additionally, the vulnerability assessments, which are utilized to identify vital areas, are based on the specifications included in the design basis threat and developed and used by the licensee to design and assess its own associated physical protection systems. Relevant scenarios are used as a basis for drills and exercises. The force-on-force exercises also include elements of sabotage scenarios.

The unclassified requirements for protection of the vital areas, as specified by the CNSC, do not define the prescriptive physical protection requirements for the vital areas, the actual physical protection measures shall be assessed and verified by the CNSC against the design basis threat.

Additionally, during the IPPAS team foot patrol-tour at Bruce Power, the team was unable to verify the actual arrangements for protection of the vital area access or protection measures due to confidentiality issues. However, the team was able to confirm that the vital areas are located inside the protected area.

Finally, the State has also defined the unacceptable radiological consequences threshold in the secret security requirements (Identification of Vital Areas for CANDU Nuclear Generating Stations) and those shall be used when identifying the vital areas.

IX.1.2. Security Plan, Including Contingency Plan

During the visit, it was explained to the IPPAS team that the licensee has a Security Plan (a Site Plan) and a Contingency Plan. These plans have been prepared in close cooperation with the local law enforcement and are consistent with the equivalent plans of the security authorities. The plans are delivered to the CNSC for acceptance as a part of the license application process. Through the *Nuclear Security Regulations* (SOR/2000/209) Section 36. (2), the contingency plans shall be verified in cooperation with the off-site response force by conducting one security exercise (force-on-force) every two years. Other joint exercises with the local law enforcement are undertaken regularly to ensure any delivery incoherence is mitigated. The IPPAS team was unable to familiarize itself with the plans to obtain more information of design, evaluation, implementation and maintenance of the physical protection system due their sensitivity. The CNSC has published a confidential, regulatory document (RD-321 Criteria for Physical Protection Systems and Devices at High-Security Sites) and the IPPAS team was informed the licensee fulfils those requirements.

An important assurance associated with the delivery of contingency planning hinges on the effectiveness of communication. In the case of Bruce Power, there are different ways to communicate with local law enforcement agencies. The principal method of two-way communication relies on a system between the Security Monitoring Room and law enforcement dispatch centre.

IX.1.3.Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety

During the visit, the IPPAS-team was informed that there are four plant operators on every shift dedicated to help emergency and security personnel in the instance of an emergency incident. This procedure has been created to ensure security personnel are aware of possible safety issues which may occur during the event. These employees also receive basic training for nuclear security to ensure potential frictions between safety and security are minimized.

Joint exercises with the security and emergency forces are undertaken regularly and the scenarios include both safety and security topics.

Additionally, Bruce Power plans for the delivery and management of integrated emergency programmes incorporating a coordination capability which is overseen by its own Integrated Response Organization (IRO). This includes assurances that there is synergy of shift systems in both safety and security disciplines. Synergizing shift patterns for both on site security and safety personnel ensures the potential for greater assurances in terms of coordination during emergency events.

Coordination of safety and security responses is managed through the site's new Emergency Management Centre (EMC). The new Mobile Operations Centre (MOC) also delivers additional opportunities for flexibility in the delivery of command and control during any nuclear emergency.

Good Practice: Operating a Mobile Operation Centre offers the potential for substantial tactical and operational command and control coherence during any security event or other nuclear emergency.

The operator has its own NMAS (Nuclear Material Accountancy System). To ensure the confidentiality, integrity and availability of the information provided by the system is accurate, the process is incorporated within the licensee's computer security programme. Nuclear Security Officers are present whenever there is an on-site movement of the nuclear material to protect it against unlawful actions. However, there are no joint exercises between the security and safeguards personnel. The safeguards department undertakes its duties quite independently from security. Cameras used for monitoring the nuclear material are not used by the security personnel. Inspecting Tamper Indicating Devices (TIDs, e.g. seals) is the sole duty of safeguards personnel. Due the nature of nuclear power plant, theft of the nuclear material is difficult (bundles are heavy and large); furthermore, the spent fuel itself provides natural protection against theft due high radiation, however, from a sabotage perspective, irradiated nuclear material itself can be a possible target.

According to NSS No. 25-G, para 2.5:
"Both the State competent authority and operator need to recognize the importance of using NMAC (Nuclear Material Accountancy and Control) for nuclear security purposes."

Suggestion: Joint activities between the safeguards and security personnel should be considered to familiarize both of each other's duties.

IX.1.4. Security Organization

The licensee maintains its own on-site response force and security organization. Security organization is located under the Law and Emergency Management (LEMS) that is directly under the Executive Team led by the President and Chief Executive Officer. There is a designated person responsible for security and emergency services (Chief of Emergency and Protective Services). Figure 8 shows the Bruce Power Emergency and Protective Services Organizational Structure. The Chief of Emergency and Protective Services has adequate authority to manage the security programme. Additionally, there are always personnel available who possess responsibility to direct security activities at the site. The Security Monitoring Room is manned 24/7

The structure of the security organization is clearly defined.

A demonstration of the tactical system underpinning regulatory requirements was evident during the IPPAS team visit to Bruce Power. Bruce Power maintains a robust and comprehensive corporate security structure, within which a separate command element oversees the delivery of emergency preparedness and response.

Bruce Power confirmed its geographic location is taken into account when formulating its emergency response and preparedness programme, and determining appropriate numbers of security personnel. Particularly, the company acknowledges that its isolation (and seasonally harsh temperatures) means self-sufficiency in security is an essential consideration. Accordingly, to prepare for a security event, Bruce Power's standard operating procedures for emergencies incorporate the coordination of four corporate entities: Security Operation; Emergency Services Operations (which include fire, medical, hazmat and rescue); Emergency Preparedness; and Support.

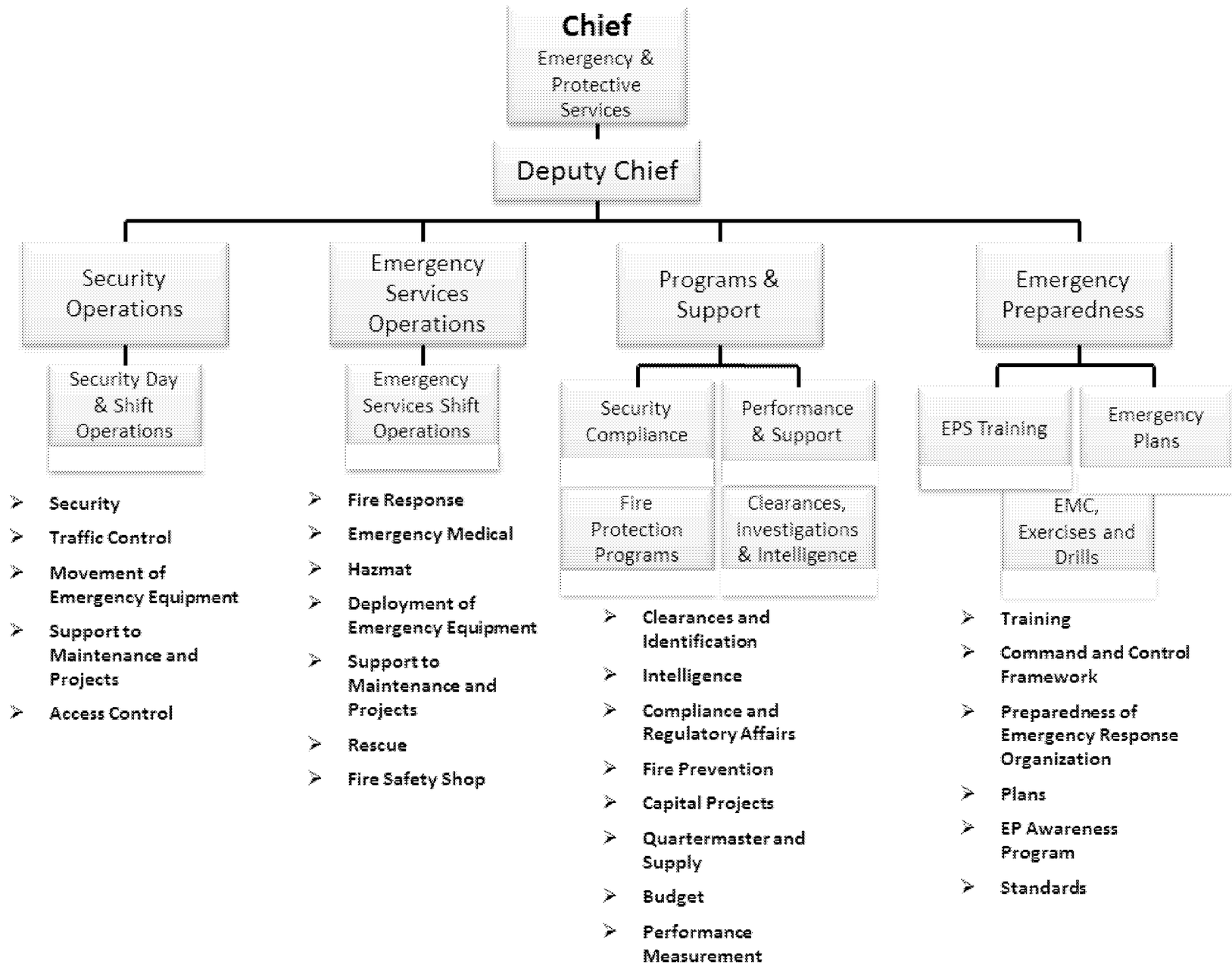

Figure 8. Bruce Power, Emergency & Protective Services Organizational Structure

The IPPAS team was informed during the visit, that the number of the security personnel is sufficient to provide a suitable level of response against any unlawful action based on the design basis threat.

IX.1.5.Security Staff Training and Qualification

The security staff receives continuous training to carry out its duties. The IPPAS team was informed on the training program in detail. Every Nuclear Security Officer receives six to seven weeks of annual training. A philosophy behind the training is “Train to excite”. The training is recorded and audited and includes a wide variety of security elements, e.g. weapons, fitness, security procedures under all weather conditions. Mandatory qualification standards for use of weapons are specified by the CNSC and these qualifications are undertaken on a regular basis. In the event that an individual fails to achieve the required standard, additional training is provided. The licensee adheres to the principles of the Systematic Approach to Training (SAT), which incorporates the following elements: analyze, design, develop, implement and evaluate. The licensee has full time instructors for different training purposes, as well as a designated coordinator for training. The training programme also engages all security personnel by requesting their input for future training activities and provides the opportunity for nuclear security officers to become Embedded Crew Trainers . This allows the licensee to ensure training is provided not only by the permanent instructors, but also by the Embedded Crew Trainers (added capacity) during the shifts. Figure 9. shows a training scenario demonstration that the IPPAS team observed as part of the review activities.

For motivation purposes and to test capabilities, the licensee engages the security personnel with other activities, for instance international competitions and challenges. Bruce Power was able to demonstrate that their teams have been very successful in such competitions.

The licensee has a separate training centre for both security and safety exercises that contains e.g. mock up turbine. There is also a shooting range on site that is used regularly for firearms training.

Figure 9. Bruce Power Training Scenario

As part of the training opportunities, the licensee has appointed members of the security organization to act as the CATT (Canadian Adversary Testing Team). These personnel receive additional training for force-on-force exercises to be carried out in other nuclear power plants in Canada.

The IPPAS team was informed that licensees' training program complies with the confidential requirements of the CNSC REGDOC/2.12.1.

The training program also includes joint exercises with the Ontario Provincial Police (OPP) which is based on the Memorandum of Understanding between the licensee and the police. There is also an exchange procedure between the licensee and the police. Under the procedure, instructors from both parties receive training from each other. Additionally, new OPP constables to the region receive introductory training of the nuclear power plant by the licensee after arrival.

The Bruce Power Centre of Excellence for Nuclear Security and Emergency Management is under development. This is a joint effort with WINS (World Institute for Nuclear Security) and other stakeholders.

Good practice: The licensee has a comprehensive training and qualifications program which ensures security staff improve and test their capabilities continuously. It engages the nuclear security officers for continuous development in a motivated way. It also provides motivation for the Nuclear Security Officers in relation to their daily routine.

Good practice: The licensee established and operates a state-of-the-art training facility which focuses on security and emergency personnel operational output.

Good practice: Between the licensee and local police department there is an exceptionally good and close working environment and relationship which ensures a robust mutual understanding of working practices and procedures. This strong relationship extends into the training domain.

IX.1.6.Security Culture

The importance of Security Culture has been recognized by the licensee. Security Awareness Training is provided to all personnel and every individual's role for the security is highlighted by management. Emergency and Protective Services hold regular intelligence briefings with safety personnel. The purpose of these briefings is to ensure managers of different departments understand the importance of the security for all operations of the licensee. By providing awareness training for all personnel and briefings for managers, the licensee is ensuring that all employees understand their role and responsibilities.

It is not apparent that the values presented in the Bruce Power's Code of Conduct explicitly recognize Security Culture. The first value of the licensee is "Safety first". Later in the Code of Conduct, security is discussed,

Suggestion:

IX.1.7.Security Procedures

The licensee has developed different security procedures for different actions and purposes. For example, procedures for patrolling the protected and vital areas, patrolling the owner controlled area (limited access area), controlling access, delivering site security clearances, car patrolling, vehicle stops all vary. Figure 10 shows a vehicle stop by security personnel within the owner controlled area. The IPPAS team was able to observe some of these procedures; for example, during the foot patrol, the team was able to observe patrolling procedure inside the protected area. During the demonstrations, the team was also able to observe procedures that are defined in the use of force (use of force continuum) and operational tactics. The procedures are documented and included in the training for Nuclear Security Officers.

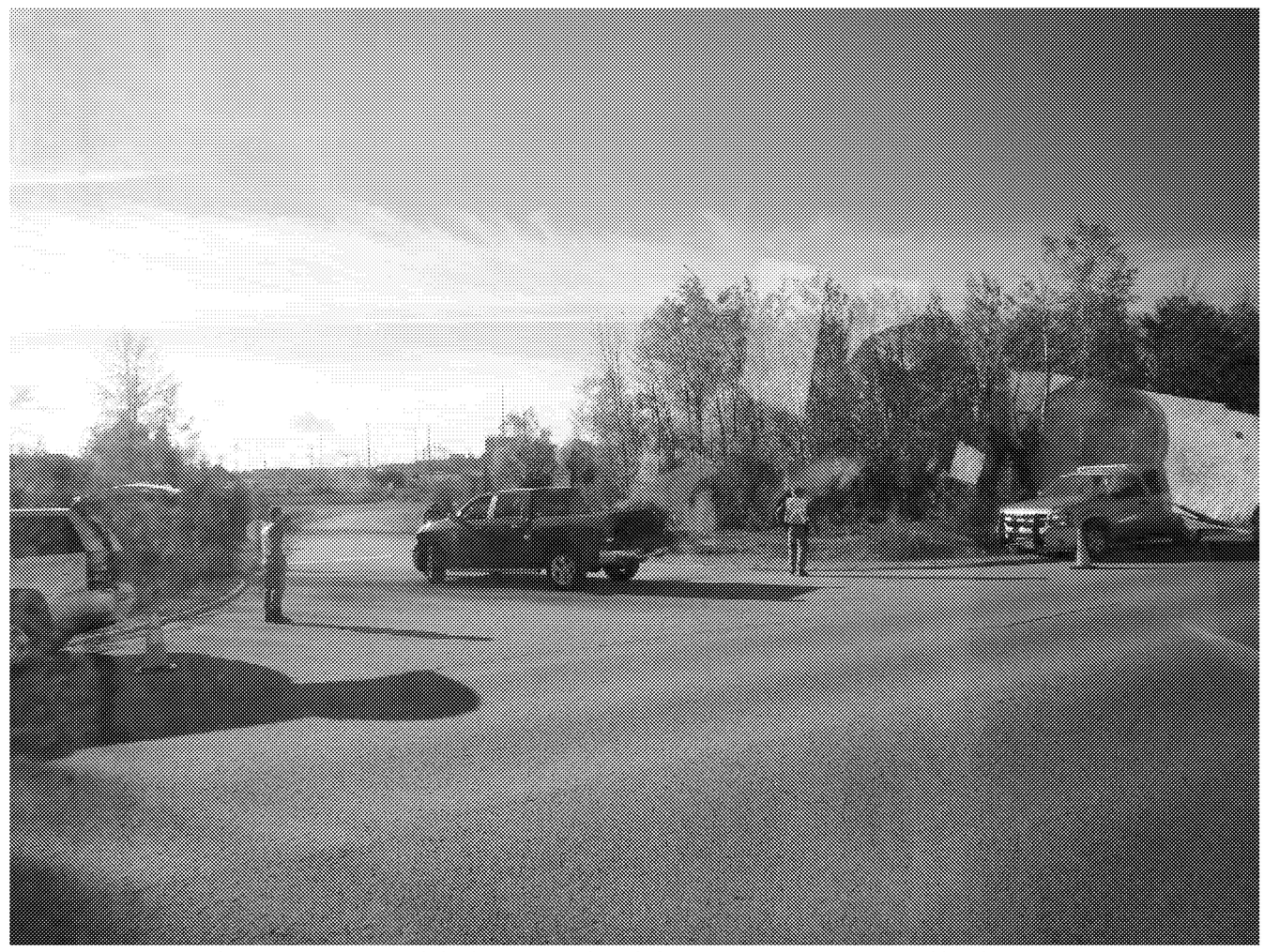

Figure 10. Vehicle stop inside Owner Controlled Area

It is a good international practice that "persons entering the protected area undergo at least random drug and alcohol testing."

Suggestion: Taking into account federal legislation, the licensee should consider performing random drug and alcohol tests for persons entering the protected area to ensure that they can effectively carry out their daily duties.

IX.1.8.Confidentiality and Trustworthiness

As part of the site access security clearance process, according to the *Nuclear Security Regulations* (SOR/2000/209) Section 42. (2), the licensee shall verify the information of the person provided by the Canadian Police Information Centre before granting the security clearance. REGDOC-2.12.2 Site Access Security Clearance provides guidance for the licensee, how to fulfill the requirement in regulations. The licensee also requires that employees self-report criminal offenses they are charged with having committed.

The licensee has a team that is responsible for conducting security clearances for employees at the site. The IPPAS team was informed about the process. After the required information of the person has been collected, the data is delivered to the Chief of Emergency and Protective Services, who makes the final decision on whether or not the security clearance is granted or denied.

The information that is related to the process is treated as confidential and stored in a security clearance process room, which is under surveillance and alarmed when unattended.
Sensitive/classified information (e.g. design basis threat), that is provided by the CNSC, is stored in a separate cabinet that fulfills the requirements. The requirements for Government classified information are derived from Security of Information Act, Policy on Government Security, Security Organization and Administration Standard, Information Security Directive and from a number of guidelines provided by the Treasury Board.

The licensee has a separate document regarding Information Classification, Access and Handling Requirements of sensitive information (BP-PROC-00110). The team was not able to observe the measures or guidelines to protect sensitive information. The recommendation in NSS No. 13 states "Information addressing possible vulnerabilities *in physical protection systems* should be highly protected."

IX.1.9.Reporting of Nuclear Security Events

According to the REGDOC-3.1.1 Reporting Requirements for Nuclear Power Plants, Annex A.1, section F, requires the licensee to report security related topics to the Commission under conditions of paras 26-30 and safeguards related topics under conditions of section G, para 31. The IPPAS team was not informed about the reporting procedures during the visit, but was told that security regulations have been fulfilled and are fully satisfactory.

IX.1.10.System Evaluation, including Performance Testing

During the visit, the IPPAS team was briefed about the Performance Testing Program (PTP). Force-on-force exercises, conducted every two years, are only one part of the Bruce Power Performance Testing Program. Additional elements for the program are procedures, regular drills and exercises, as well as a maintenance program of physical protection systems. Joint exercises with off-site response forces are an important part of the performance testing, because they cover both on-site and off-site response for security events. The annual Threat and Risk Assessment helps to identify possible gaps in performance. Modifications required after the assessment are verified by the CNSC.

Bruce Power also operates and manages a sophisticated and comprehensive 3-D modelling programme (incorporating both internal and external modelling of its facilities). This modelling supports the (regularly-updated) Tactical Deployment Plan.

Good Practice: Development and utilisation of a comprehensive 3-D modelling of the facilities allows very substantial opportunities for tactical awareness and understanding on the part of any response force and support the development of tactical deployment plans.

IX.1.11.Quality Assurance

Quality assurance at the facility is done through procedures and maintenance program. Bruce Power conforms to CSA N286-05 Management System Requirements for Nuclear Power plants as the standard which integrates quality requirements with other requirements such as health, security, radiological, business etc., while ensuring safety is the overriding consideration guiding decisions and actions. The licensee uses the PDCA Cycle model (Plan – Do – Check – Act), similar to ISO 9000 standards. A system performance criteria has been defined, and a preventive maintenance program is in place. The licensee defines how the testing of physical protection systems shall be delivered and, if required, corrective actions shall be taken. An internal peer review system has been created to ensure that the programs are followed. The IPPAS team was not able to familiarize or assess the documents due to the short duration of the visit.

IX.1.12.Sustainability Programme

During the visit, the IPPAS team was not made aware of a sustainability programme. However, some elements such as the maintenance programme were evident and explained to the IPPAS team.

A program for security improvement actions exists in practice. During the gap analysis and through the TRA, the licensee identifies possible gaps and makes corrective actions, if needed.

The Plan-Do-Check-Act cycle ensures program sustainability through continuous monitoring of performance and incorporating areas of improvement into the business planning cycle. There are three levels of program assessment: operational activities performed on a daily basis; planned program assessment activities that are established in the annual improvement plan, some of which include independent audit, and external assessment activities. The outputs of assessment activities are documented in the corrective action program and where risks are identified, recorded in the company risk register. The annual business assessment process includes an "Excellence Plan" which drives the continuous improvement through initiatives, capital projects, organizational evolution and management system updates.

During the visit, the IPPAS team was informed about recruitment processes. For several open positions there are usually approximately 500 applications. Accordingly, the licensee is able to select high quality personnel from the multiple applications it receives. Former employment history, as well as background education are required from the applicants. The CNSC has also published REGDOC 363 for certification of a Nuclear Security Officer and confidential, regulatory document REGDOC-2.12.1 (High Security Sites: Nuclear Response Force). The licensee applies the requirements specified in these documents.

Finally, the PPAS team gained assurance that Bruce Power maintains an ongoing modernisation and procurement programme which benefits the emergency response capability, specifically in terms of Detection and Delay. Over the past five years, Bruce Power has delivered upgrades

IX.2. Physical Protection System (PPS)

IX.2.1. Graded Protection and Defence in Depth

The Bruce Power site contains four protected areas: Bruce A and Bruce B nuclear power plants, Douglas Point Waste Management facility and the Western Waste Management Facility and numerous other buildings or working areas. Each of these four nuclear facilities is located within a dedicated protected area that is located inside the owner-controlled area (OCA) (limited access area).

Bruce Power operates an integrated, comprehensive physical protection system which incorporates the principles of a graded approach to security and defence-in-depth, including Security Monitoring Room (SMR), protected areas and their related vital areas, an on-site response force supplemented by an off-site responses force. A tour of the Bruce Power site afforded the IPPAS team opportunities to observe main entrance gate at the Owner Controlled Area (OCA) (Limited Access Area), an external overview of the Bruce A protected area fences and a visit of the Bruce B protected area, including associated access control. The IPPAS team visited the Security Monitoring Room

IX.2.2. Detection

Owner Controlled Area (Limited access area)

The outer perimeter is defined as the OCA. The IPPAS team was informed that the site is surrounded by a simple perimeter fence.

Warning signs are fitted on the OCA perimeter fence to deter unauthorized access as shown in Figure 11.

Figure 11. Warning signs on OCA perimeter fence

Each authorized person entering the site must have their badge issued by Bruce Power. The visitors and other non-permanently authorized person must be escorted.

At the main gate, the team observed the entry process for visitors and authorized personnel and the search procedure for vehicles. The main gate is staffed 24/7. Staff vehicles entering the OCA must have a vehicle sticker and a valid badge. Visitors must provide a valid identification and have sponsorship prior to access onto the site.

The IPPAS team was informed that two others gates are located at the OCA boundary for entrance and exit at rush hours. When not in use, the gates are secured and monitored.

Part of the protected area of Bruce A and B, and the OCA boundary runs close to the shore of Lake Huron. The IPPAS team viewed the exterior of Bruce A facility and its protected area boundary whilst standing close to the lake. The team was able to gain assurance that potential ingress opportunities utilizing the lake had been identified and blocked.

Bruce Power contracts K-9 services quarterly to conduct searches. Searches for explosives and drugs are conducted on a random basis in locker rooms, access control areas, and vehicles on the site.

Protected areas

During the tour, the IPPAS team visited the Bruce B protected area and undertook an external observation of the physical barrier (chain-link fences topped with concertina wire and a clear isolation zone) at the protected area boundaries.

At Bruce A, the team undertook an external observation of the same capabilities. The fences at both facilities and related equipment appear in good condition and an unobstructed area was maintained on both sides of the fence to allow assessment by guards or cameras.

Marine exclusion barriers have been installed to prevent unauthorized access by water as shown in Figure 12.

Figure 12. Marine exclusion barrier

Jersey barriers surround the protected areas' fence to prevent vehicle penetration into the protected area. Where Jersey barriers cannot be installed, aircraft cables have been incorporated. A full analysis of the vehicle risk was conducted and the barriers were designed using the DBT.

The IPPAS team followed a full foot patrol by Nuclear Security Officers inside the building housing the Units 5 to 8 of the Bruce Power nuclear power plant. During this foot patrol, one of the Nuclear Security Officers visited the main control room (MCR) while the IPPAS team stayed in the

hallway in front of the door used by this Nuclear Security Officer. The team was provided information on access controls and physical protection systems in place for the MCR. However, the IPPAS team was not able to gain access into these rooms or observe the related access control procedures.

Vital areas

The IPPAS team was informed that a vulnerability assessment was conducted at the Bruce Power Nuclear Power Plant to identify and appropriately protect the vital areas in accordance with regulatory requirements.

Nevertheless, because during the visit the IPPAS team did not observe the physical protection provisions or procedures in place at vital areas, the IPPAS team was not able to assess the physical protection measures.

IX.2.3. Access Control

The IPPAS team observed the access control process when entering the Bruce B protected area for personnel, bags and packages. The access control area is manned by armed Nuclear Security Officers 24/7. Persons entering the protected area are required to go through a multi-layered physical security infrastructure which includes:

After successful completion of these controls, access is allowed into the protected area through a turnstile followed by radiation monitoring. A ballistic guard booth is located within the access control area providing observation of the internal access control and vehicle portal. Additionally, the detection systems incorporate scanning for some mobile electronic devices.

Good practice: The use of systematic checks for all entrants to protected areas is a good practice.

Figure 13. Access Control Area at Bruce B Protected Area

The procedure in force for vehicle searches was also presented to the team. There is a vehicle portal for the screening of vehicles when entering and exiting the protected area. The portal gates are interlocked so that they can only open one at a time. The Nuclear Security Officer undertakes the vehicle search

The IPPAS team was informed about the access authorization database which is updated in a timely manner in order to allow Bruce Power to revoke authorization immediately for any individual whose employment is terminated.

Suggestion:

The IPPAS team was informed of the key control procedure (DIV-EPS-00403) operated by the licensee. The objective of this document is to provide Bruce Power Security personnel an overview of the key control procedure. The requirements related to key control are defined in the Nuclear Security Regulations (SOR/2000/209) Section 15.2. Procedures operated by the licensee fulfill these requirements. It was explained to the IPPAS team that keys for security patrolling are maintained in the "Keywatcher" keytels

Following a review of the Bruce Power key control procedure document, some inconsistencies were identified. In a number of cases, the word '*should*' was used instead of 'must' or 'shall'. For example, in section 4.2.4 Master Keys it states: "*Careful records of such issuance should be kept by Lock & Key Specialists. The list should be reviewed periodically to determine whether all those authorized should continue to hold such keys.*"

IX.2.4. Security Monitoring Room (Central Alarm Station)

The team visited the Security Monitoring Room (SMR), which is located
The SMR monitors and services the entire site. Bruce Power indicated that two back-up SMR's
Each of these back-up SMR's can substitute the SMR and can be staffed and operated very quickly.

The SMR was renovated in 2015 with new alarm detection and presentation subsystem and a new video management system. The SMR is staffed permanently by nuclear security officers and appears appropriately equipped to provide suitable levels of alarm display and assessment. Uninterrupted power supply is provided by a generator and back-up batteries. All assessment and monitoring alarms are tamper protected. A variety of communication methods are in place and the Bruce Power team explained that (in order to satisfy regulatory requirements), they operate three separate communication systems including encrypted radios, landline and satellite phones. Additionally, the SMR had direct communications with the Ontario Provincial Police dispatch center and control room. Radio checks are conducted every shift for onsite and off-site radios. This SMR integrates a tactical command room.

The section 15 of the Nuclear Security Regulations SOR/2000-209 does not require threat and risk assessment for SMR. CNSC indicated to the IPPAS team that the SMR fulfilled the regulatory requirements.

IX.2.5. Delay

The nature of the physical barriers surrounding the protected areas are two chain-link fences topped with concertina wire providing an isolation zone The IPPAS team was not provided an opportunity to visit a vital area, therefore a determination on the adequacy of the delay measures cannot be made.

IX.2.6. Response

Response to security events is provided by the Nuclear Security Officers in Nuclear Response Forces belonging to Bruce Power Emergency and Protective Service and by off-site law enforcement (provided by the Ontario Provincial Police).
The on-site Nuclear Response Forces resources were presented to the IPPAS team. During the visit, Bruce Power displayed and demonstrated equipment and assets including armament and ammunitions, individual protection, communication means and vehicles to the IPPAS team. The IPPAS team was told during the visit that there is a process for recognizing proper equipment for the Nuclear Security Officers that involves the members of Nuclear Response Forces. A separate team of experts evaluate the new equipment before they are introduced to the CNSC and the management. This process also includes variety of testing of possible new equipment to ensure they are adequate for the response forces. Additionally, the facility utilizes a number of light armored vehicles for patrolling and both mobile and static surveillance and reconnaissance purposes. The IPPAS team considers that the on-site response force is very well trained and qualified to carry out its duties (see section IX.1.7).

The IPPAS team noted that the Bruce Power Nuclear Response Force was well resourced, robust and demonstrated high standards of training. The IPPAS team assesses that such high standards are necessary to ensure that potential vulnerabilities stemming from the wider site are mitigated.

The IPPAS team noticed also that force on force exercises satisfied the CNSC requirements.

Balanced protection

To ensure effectiveness of protective security systems, a balance between the critical functions of Detection, Delay and Response is essential. Bruce Power's physical protection system is comprehensive, multi-layered and incorporates these principles.

However, while the IPPAS team's exposure to the physical protection measures operating in the wider Owner Controlled and Protected Areas was substantial, an understanding of the balance between these three critical protection concepts was hampered by a limited understanding of the security systems and procedures in place at the Bruce Power Vital Areas.

Force-on-force exercises, including in the OCA, are conducted in order to evaluate the balance between detection, delay and response and validate performance objectives are met. All alarms are timed and tracked by the licensee to ensure performance objectives are achieved. Bruce Power is developing a security assessment software tool to evaluate response strategies

X. NUCLEAR RESEARCH REACTOR AT McMASTER UNIVERSITY

This chapter of the report mainly covers the security of the McMaster Nuclear Reactor (MNR), but it also addresses some aspects related to security of the sealed radioactive sources available at McMaster University.

McMaster University is medium sized, research intensive University situated in Hamilton, Ontario (80 km West of Toronto). McMaster University boasts approximately: 23,000 full time undergraduate students, 3,000 graduate students, 7,000 staff and faculty members. Research Funding is about $400M annually. McMaster Nuclear Reactor is the epicentre of the extensive nuclear science-related facilities on campus that mark McMaster as Canada's Nuclear University.

The McMaster Nuclear Reactor (MNR) began operating in 1959 as the first university-based research reactor in the British Commonwealth. By design, MNR was 5 MW (currently 3MW) pool type reactor with full concrete containment structure (see figure 14 below). Initially, MNR was operated using HEU fuel, but in 2007 was converted to LEU fuel. MNR operates 5 days a week16 hours per day and its operating efficiency is 85%.

MNR is one of the world's largest suppliers of the medical radioisotope iodine-125 which is used for the treatment of prostate cancer. It also produces other medical and industrial isotopes.

In addition to the MNR, the suite of facilities located at McMaster University includes a Taylor Source ~20TBq Cs-137 large field irradiator (category 2 source), one cyclotron, three linear accelerators, three gamma cell irradiators (category 2 sources) and radioisotope laboratories. There are also other holders of small amounts of nuclear material on the campus. One hot cell is in operation at MNR and several new hot cells have been installed at the laboratories and are currently being commissioned, but will be licensed to handle nuclear material. The location map of MNR and other facilities hosting high activity radioactive sources is provided in Figure 14 below.

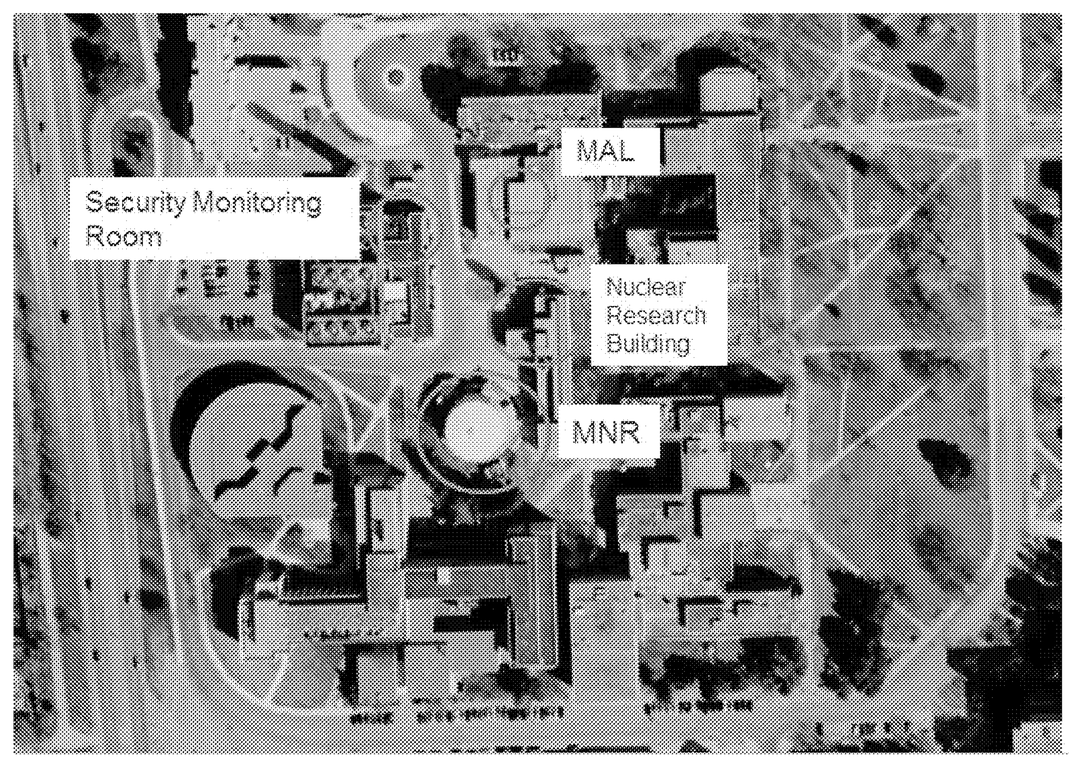

Figure 14. Map of MNR and Associated Facilities

The IPPAS team's visit to McMaster University was mainly focused on the security of the MNR and high activity sealed radioactive sources. The team was briefed by the management of MNR and discussed issues related to the University's corporate and MNR's security as well as security of high activity sealed radioactive sources located on the McMaster University Campus. The team held a

questions and answers session and conducted a tour of the MNR, Security Monitoring Room and the Taylor source irradiator. The team also met the representatives of McMaster Security Services and Hamilton Police and discussed their roles and responsibilities as well as other issues related to security of MNR and high activity radioactive sources. Due to the short time of the visit, team was not able to see other high activity sealed sources and observe the physical protection measures in place.

X.1. Security Management Programme

X.1.1. Threat and Target Identification

The MNR is operated using the LEU fuel, which is Category III nuclear material according to NSS NO. 13.

X.1.2. Security Plan, Including Contingency Plan

The IPPAS team was informed that, in accordance with the CNSC requirements, vulnerability, threat and risk assessments have been conducted for the MNR, including for insider threats. MNR has developed a security plan and contingency plan, which was accepted by the CNSC, to fulfil the requirements for a Class 1A Non-Power reactor operating licence facility as specified in the CNSC Nuclear Security Regulations. The details of the security and contingency plan were not provided, but the IPPAS team was informed that they are fully consistent with CNSC regulations.

X.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety

Both safeguards and security procedures are associated with each fuel movement. The Director, Nuclear Operations and Facilities (DNOF) is responsible for nuclear security and safeguards, as specified in the job description for that position. The inherent safety features of the reactor and containment building also reduce the vulnerability of the reactor to sabotage.

X.1.4. Security Organization

The President (and Vice Chancellor) of McMaster University is the CNSC license holder for the all of the university's licensable facilities and materials, including the MNR and sources held by the university.

The DNOF is responsible for nuclear security and works in liaison with Director of Security and Parking, Security Services Department, who is in charge of corporate security, and the Senior Health Physicist, Health Physics Department to establish and manage the MNRs nuclear security system. DNOF reports directly to the Vice-President for research of the University. Some tasks such as the issuing of security passes involve corporate areas of MNR.

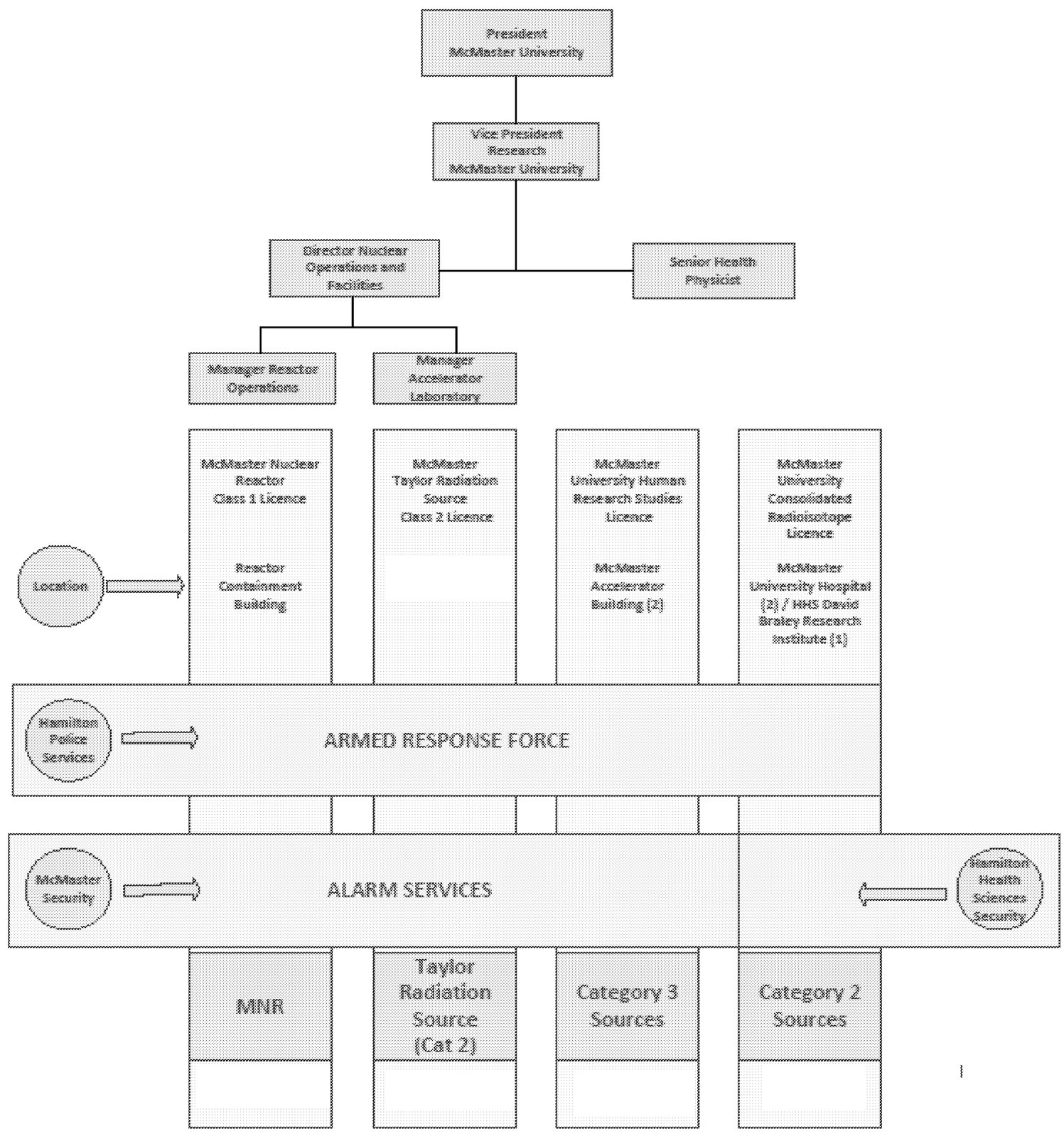

Figure 15. Organisation chart for MNR highlighting security responsibilities

X.1.5. Security Staff Training and Qualification

Initial and ongoing security awareness training is provided for staff with access to the MNR. McMaster University special constables (peace officers) provide guarding services for the whole university including the MNR. They are trained by Hamilton Police Service. It was evident through discussions that significant resources are allocated to training and awareness. The DNOF is very experienced in nuclear security practices.

X.1.6. Security Culture

Based on the information provided during the briefings and discussions, it was evident to the IPPAS team that importance of security is strongly recognized by the management and employees of the MNR as well as at corporate level of McMaster University. The same extends to the recognition of the credible threats.

The McMaster University security mission statement is posted on its web-site which states that it's the responsibility of the entire community to develop a safe and secure environment at the university.

Security culture at the MNR is established through initial security induction, ongoing awareness training and enforcement (including loss of access privileges) in a graded approach, depending on the access available to staff. General campus security awareness features in the induction material for new students at the university and includes specific reference to the MNR. Students are sensitized to report suspicious behaviour on the campus and have done so.

X.1.7. Security Procedures

In the course of the visit, reference to a number of security related procedures were mentioned, for example: for tours and visits to the MNR, fuel movements, daily reactor shutdown, issue of security badges, and response and communication instructions for the SMR operator. The IPPAS team was not able to review the contents of these procedures, but it believes that MNR's set of procedures addresses all important security areas.

X.1.8. Confidentiality and Trustworthiness

The MNR security and contingency plan and other associated information are treated as prescribed information in accordance with the General Nuclear Safety and Control Regulations and are protected accordingly. There was a clear awareness to the need to control access to sensitive information during the visit to MNR. The security network is separate to other campus networks and is not facing the internet. MNR's security plan is stored in a secure container in accordance with CNSC requirements.

Trustworthiness checks are conducted for persons granted unescorted access to the MNR, in accordance with CNSC requirements.

Four staff have high level security clearances enabling them to receive current threat information as required. MNR staff undergo supervisory awareness training providing a level of ongoing monitoring of trustworthiness.

X.1.9. Reporting of Nuclear Security Events

The MNR has recently installed a programmed automatic call-out contact system to assist the implementation of emergency response procedures, which avoid a single person having to separately call multiple first responders. The Director, Nuclear Operations and Facilities was aware of licensee responsibility to promptly report security events verbally to CNSC and thereafter to lodge written security events notices and follow-up reports.

X.1.10.System Evaluation, including Performance Testing

The MNR conducts an annual table-top exercise and security drills of specific security scenarios. Lesson learned are recorded and followed up as appropriate. Security procedures are purposely tested during non-nuclear emergencies and exercises (e.g. fire). The SMR equipment is tested monthly. Together these display a strong commitment to maintaining a robust security system.

X.1.11.Quality Assurance

The MNR employs a Quality Management System for document control, including those associated with nuclear security plans and procedures.

X.1.12.Sustainability Programme

The MNR is fully funded by commercial activities which provide the means to fund its security requirements, however McMaster University overall has strong commitment to the safety and security of students on campus which supports well MNR's specific security requirements. Team was told that the security budget competes with safety investments and with other priorities that are regarded as essential to the university community. Nevertheless the recent investment in an upgraded SMR (see below) for instance shows a strong commitment to nuclear security.

A preventive maintenance programme is established and implemented. The maintenance of security equipment (e.g. cameras) is done according to a maintenance schedule.

X.2. Physical Protection System (PPS)

The MNR's physical protection system is integral part of the corporate security system of the University. It is also important to mention, that after the MNR's conversion from HEU to LEU fuel some of the configuration features of the security system originally in place for the protection of HEU, remains in place.

X.2.1. Graded Protection and Defense in Depth

Figure 16. MNR Pool

X.2.2. Detection

X.2.3. Access Control

X.2.4. Security Monitoring Room (Central Alarm Station)

The recently upgraded SMR is located in an above-ground level room in a building outside of reactor containment.

There is also a backup SMR providing 100% redundancy which is tested for operability once per month. Contingency plan include procedures for scenarios in which

Such a modern SMR setup (including backup) for such a facility is impressive.

Figure 17.

Figure 18.

MNR's SMR at McMaster University

The university has a dedicated command post elsewhere on the campus which is activated during emergencies and coordinates with the SMR as required.

X.2.5. Delay

X.2.6. Response

On-site response to security events is done by campus guards (special constables/peace officers) which are trained by Hamilton Police Service. As required, off-site response can be escalated

through Hamilton Police Service, then emergency resources at provincial and federal levels. MNR provides annual orientation of the reactor for security services and local tactical police for higher risk facilities.

There is a MoU in place between McMaster and the Hamilton Police Service for the provision of assistance should a security events escalate beyond the capability of the Special Constables to resolve. It was evident during the visit that there is a very strong, interactive and mature relationship between the MNR management, McMaster security and local police services, as they often meet, exchange expertise providing strong situational awareness. This is the cornerstone of security posture at McMaster. The IPPAS team appreciated the time taken by Hamilton Police to accompany the tour.

McMaster University has developed a mobile phone application called MUSST (McMaster University Safety, Security and Transit), available to all persons, which provides campus security and emergency response instructions including specific information regarding the McMaster Nuclear Reactor. The application *also* provides for the sending of information (e.g. photos) directly to campus security. All public security procedures are available through this app. It has several security-related features including for example instructions on reporting suspicious packages. McMaster considers this app as just a start, and is planning to include even more (security-related) features. The IPPAS team considers this app and this initiative as a good practice and encourages McMaster in its further development.

Good Practice: The McMaster University campus phone application MUSST (McMaster University Safety, Security and Transit) provides important security and emergency response information including for the McMaster Nuclear Reactor.

Overall, MNR and McMaster University together have well met the challenge of balancing a strong security posture and culture while maintaining academic openness and transparency. The effort to engage the entire campus community to play a part in security has paid sound dividends.

X.2.7. Radioactive Source at McMaster – Taylor Source

The IPPAS team observed security arrangements for one radioactive source, namely a category II cesium-137 Taylor source. Under CNSC security regulations the Taylor source is a Class 2 facility. Other radioactive sources on campus such as gamma cells were not visited. The overall security system for the source (including the SMR) is the same as that in place for the MNR.

XI. WESTERN WASTE MANAGEMENT FACILITY OF ONTARIO POWER GENERATION

This chapter addresses security of the Western Used Fuel Dry Storage Facility (WUFDSF), which is operated by Ontario Power Generation (OPG) and was visited by the IPPAS team during the mission.

OPG has been incorporated since 1999 and is the successor company of Ontario Hydro. OPG's assets currently includes two nuclear generating stations (Pickering and Darlington), three used fuel dry storage facilities (UFDSF), which includes Darlington, Pickering, and the Western Waste Management Facility consisting of the WUFDSF and Low and Intermediate Level Waste Storage facility situated at Bruce Power Site.

The WUFDSF is located within a separate protected area within the Western Waste Management Facility and is comprised of a processing building and four storage buildings. WUFDSF's current team is comprised of 39 staff and processes over 100 dry storage containers (DSCs) annually.

During the visit, the IPPAS team was focused on the security of the WUFDSF and did not review the security of the Low and Intermediate Level Waste Storage facility. During the visit, the IPPAS team also discussed security arrangements for the transport of used fuel from the Bruce Power station B to the WUFDSF, and was able to observe the vehicle, which is used for transport of used fuel.

XI.1 Security Management Programme

The Security Management Programme operated by OPG covers the following areas: threat and target identification, structure and elements of security organization, interfaces with nuclear material accountancy and control and nuclear safety, reporting of nuclear security events and system evaluation and performance testing.

XI.1.1. Threat and Target Identification

The CNSC produces and provides the Design Basis Threat to the facility operator. According to the Nuclear Security Regulations (SOR/2000/209) Section 7.4 (2) the Commission shall provide a current design basis threat analysis to every licensee, who shall take that analysis into account. Section 7.5 (1) requires every licensee to conduct a threat and risk assessment (TRA) specific to that facility at least every twelve months. It is also required by the CNSC that modifications shall be undertaken by the operator in respect to the TRA.

The Nuclear Security Regulations (SOR/2000/209) Section 14.1 requires the licensee to identify all vital areas taking into account design basis threat and other relevant information. During the visit the IPPAS team was not provided information related to TRA, but the nature and use of the facility itself explains possible targets. The State has also defined the unacceptable radiological consequences (URC) threshold in the secret security requirements (Identification of Vital Areas for CANDU Nuclear Generating Stations) and those shall be used when identifying the vital areas.

Because the WUFDSF is classified as a High Security Site as defined in the Nuclear Security Regulations, the physical protection measures equivalent to the nuclear power plants are

undertaken. It was explained to the IPPAS team during the visit that all requirements are rated fully satisfactory.

XI.1.2. Security Plan, Including Contingency Plan

The IPPAS team did not receive information during the visit in regards to a Security Plan or Contingency Plan, however those are requirements by the CNSC that are fulfilled by the licensee. Under the Bruce Site Services agreement, Bruce Power conducts regular drills and has a contingency plan in place to respond to events within the WUFDSF.

XI.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety

The operator has its own NMAS (Nuclear Material Accountancy System). There is a stand-alone computer for NMAC (Nuclear Material Accountancy and Control) that is accessible only for those persons, whose duties include filing the information into the system. There are also IAEA (International Atomic Energy Agency) cameras installed. These cameras are operated solely by the IAEA and the licensee fulfils international safeguards agreements obligations. The licensee operates its own NMAS that contains accurate data of nuclear material. During the process, the DSCs (Dry Storage Containers) are under constant supervision by the staff until the DSC has been welded. After welding it takes an extensive amount of time to open the DSC again, therefore once the spent fuel has been stored in the DSC, retrieval cannot occur without being noticed by the staff. The DSCs are sealed by the IAEA after welding and verification and the seals are monitored by the IAEA inspectors regularly.

XI.1.4. Security Organization

The on-site response force is provided by the Bruce Power under the Bruce Site Services agreement. There is a designated person responsible for security by the licensee. This person has authority to manage the security programme. Additionally, there are always personnel available who possess responsibility to direct security activities on the site. The Security Monitoring Room is located on the Bruce site and is

The structure of the security organization is clearly defined.

Outside of office hours, security is provided by the Bruce Power's security organization that patrol at the area under the agreement of the licensees.

It was explained to the IPPAS team during the visit that

XI.1.5. Security Staff Training and Qualification

The security staff is provided by Bruce Power, therefore the same training and qualification program applies. The security organization receives continuous training to carry out its duties. The training is recorded and audited and includes a great variety of security elements, e.g. weapons, fitness, security procedures under all weather conditions. Mandatory qualification standards for use of weapons are specified by the CNSC and these qualifications are tested on a regular basis. In the event that an individual fails to achieve the required standard, additional training is provided.

It was explained to the IPPAS team that the nuclear security officers providing security and performing the access control checks

Most of the nuclear security officers on-site, however, receive firearm training and are qualified for the equipment.

XI.1.6. Security Culture

The importance of Security Culture has been recognized by the licensee. There is a Continuous Behavioural Observation Program (CBOP) and supervisors are required to take this training. There is also a Partnership and Security Awareness program, creating a Security Culture through the whole OPG. The motto is "Security is everybody's business." On the OPG's (Ontario Power Generation) website there is a statement: "Safety and security are engrained in OPG's culture." However, the Code of Business Conduct (Jan, 2015) recognizes as values: Safety, Integrity, Excellence, People & Citizenship, but no security. Figure 19 lists OPG's mission, values and behaviors.

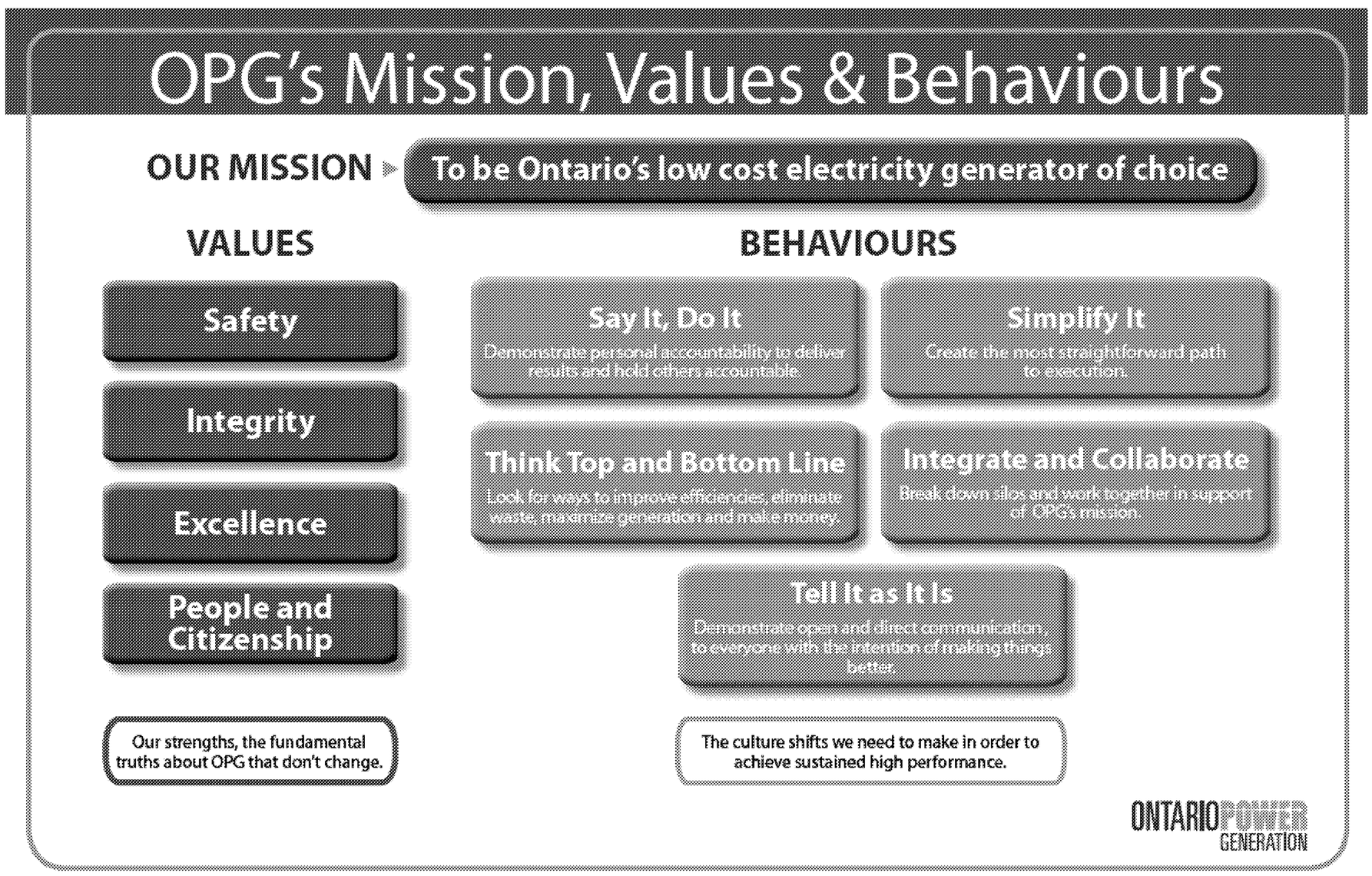

Figure 19. OPG's Mission, Values & Behaviors

Suggestion: To further promote the importance of Nuclear Security Culture, the licensee should consider formally enshrining its importance by explicitly referring to nuclear security culture, e.g. in its values of Code of Business Conduct.

XI.1.7. Security Procedures

During the visit, the IPPAS team was able to observe the access and exit control procedures at the facility. The security procedures are carried out by the Bruce Power personnel who have written instructions for patrolling during outside of office hours. Other procedures are agreed by the two licensees. During the visit the IPPAS team was briefed on OPG's security program that is implemented through Standards, Procedures and Instructions. These are regularly communicated for procedural use.

XI.1.8. Confidentiality and Trustworthiness

The OPG's governance prescribes standards for the transmittal, storage and disclosure of sensitive information. It also covers the information related to security in electronic form that is stored and transmitted encrypted.

The sensitive information that is provided by the CNSC is protected under the requirements by the CNSC and inspected by that Authority. The requirements for Government sensitive information (e.g. design basis threat) are derived from Security of Information Act, Policy on Government Security, Security Organization and Administration Standard, Information Security Directive and from a number of guidelines provided by the Treasury Board.

Under the Bruce Site Services agreement, Bruce Power conducts the trustworthiness checks, because they are providing the access badges to the WUFDSF. The procedure fulfills the requirements in REGDOC-2.12.2 Site Access Security Clearance. The final decision whether or not the access is granted is done by the licensee (OPG).

XI.1.9. Reporting of Nuclear Security Events

According to the GNSCR, section 29 licensees are required to report security breaches to the Commission The IPPAS team was not briefed about the reporting procedures during the visit, but was informed that security regulations have been fulfilled and are fully satisfactory.

XI.1.10. System Evaluation, including Performance Testing

During the visit it was explained to the IPPAS team that Bruce Power provides the on-site response and performs daily security duties, as well as Bruce Power's Performance Testing Program. Security administration is provided by Bruce Power under the OPG's contract agreement.

Force-on-force exercises conducted every two years are only one part of the Bruce Power Performance Testing Program. Additional elements for the program are procedures, regular drills and exercises, as well as a maintenance program of physical protection systems. Joint exercises with off-site response forces are an important part of the performance testing, because they cover both on-site and off-site response for security incident. The annual Threat and Risk Assessment helps to identify possible gaps in performance. Modifications required after the assessment are verified by the CNSC.

A responsible system engineer (RSE) reporting to OPG performance engineering is accountable for the performance monitoring of security system components. The system is maintained by facility control technicians who are security cleared to the equivalent of Federal Government Secret (Level II). Intrusion detection devices are tested weekly by the Nuclear Security Officers.

XI.1.11. Quality Assurance

There is an accountable manager for the security program at WUFDSF. The Agreement between Bruce Power and OPG, that contains details of provided security services, is monitored through regular communication, quarterly interface meetings and formal and informal self-assessments.

XI.1.12. Sustainability Programme

The IPPAS team was briefed about the maintenance program (see above under XI.1.10), but the other elements of the sustainability programme were not introduced to the team due to the short duration of the visit.

XI.2. Physical Protection System (PPS)

The IPPAS team toured the Western Used Fuel Dry Storage Facility (WUFDSF) on the Bruce Site. According to the Nuclear Security Regulations, this facility is considered a "high security site" and the physical protection system must be designed accordingly.

A comprehensive presentation of the physical protection system was delivered to the IPPAS team by the Security and Emergency Service of Ontario Power Generation.

The IPPAS team visited the protected area and the dry storage buildings.

XI.2.1. Graded Protection and Defence in Depth

The WUFDSF is within a protected area, inside the site of Bruce Power. The WUFDSF has radiological and security boundaries, the other nuclear facilities (Low and intermediate waste storage) have only radiological boundaries.

XI.2.2. Detection

The perimeter of the protected area is surrounded by a fence equipped with

XI.2.3. Access Control

Persons requiring access to the protected area must first pass through an explosive substance portal detector (see Figure 20.) and carry a proximity card including their photo allowing verification of identity. Access verification is achieved by two separated tracks: After positive identification, access is provided through a turnstile as shown in Figure 21.

Good practice: The use of systematic explosive substance checks for all entrants to protected areas is a good practice.

Figure 20. Explosive Substance Portal Detector at Protected Area Entrance

The IPPAS team entered the protected area and was able to observe the access process and the related searches for detection of prohibited items.

The vehicle entrance into the protected area contains a vehicle search portal which isolates the vehicle during search. Searches include use of portable explosive detection, hand held metal detector and baggage inspection.

Figure 21. Turnstile at the Protected Area Entrance

The facility is alarmed and under CCTV surveillance. All alarms are announced at the SMR and the Nuclear Response force takes appropriate action.

XI.2.4. Security Monitoring Room (Central Alarm Station)

The management of detection and all related activities relay to the Bruce Power SMR. The two back-up stations at provide full redundancies of the SMR including the Western Waste Management Facility. See section IX.2.4.

XI.2.5. Delay

Outside the protected area an underground pathway is protected against intrusion by honeycomb steel pipes and in combination with random security patrol and CCTV assessment.

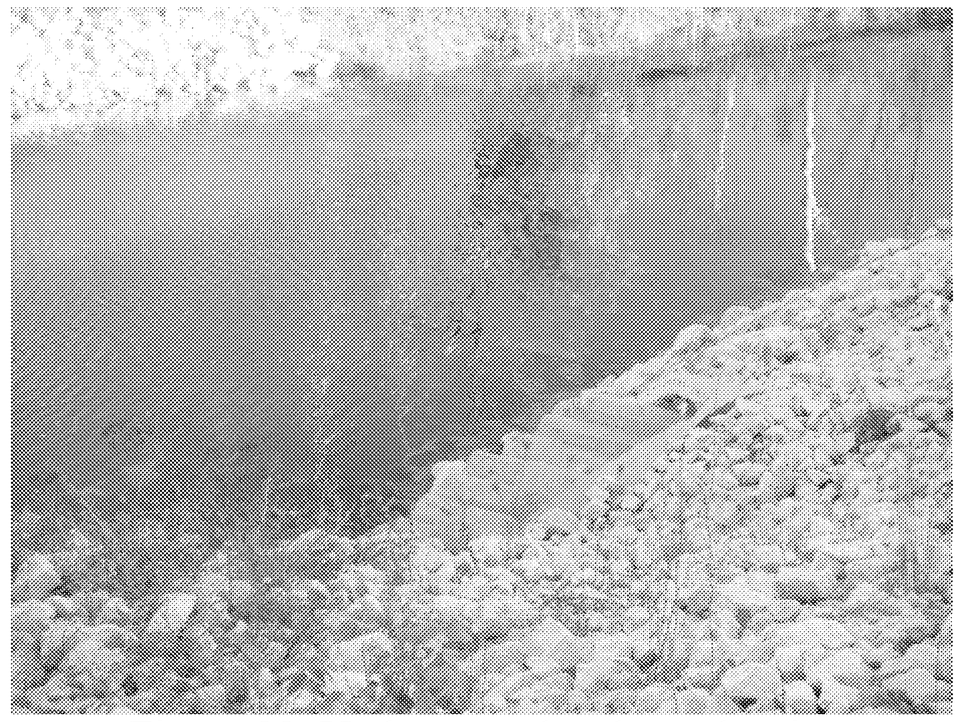

Figure 22. Underground pathway barrier

The delay provided by the fence at the protected area itself is limited. Additional delays at the protected area are provided by a continuous "Jersey Concrete" barrier to counter forced vehicle penetration. Further delay to the protected area is provided by an underground pathway barrier as shown in Figure 22. At the vehicle entrance to the protected area an active vehicle barrier is in place as shown in Figure 23.

Figure 23. Vehicle barrier at the Protected Area

Inside the dry storage buildings more than 1000 Dry Storage Container (DSC) are stored which are, for safety purpose, very robust and heavy. The containers are of significant construction of high-density concrete and are lined outside with steel plates and welded shut. When the container is full and welded shut, the weight is over 70 metric tonnes. The IPPAS team believes the containers provide sufficient delay against malicious acts.

XI.2.6. Response

Response is provided by Bruce Power as described in section IX. Bruce Power has a MoU with the Ontario Provincial Police to provide an off-site response force to the Bruce Power Site. Ontario Power Generation has a written agreement with the OPP to extend this service to OPG facilities within the Bruce Power site. Bruce Power Security patrols provide 24/7 response to alarms or events.

As a result of the information received and observations on the site, the IPPAS team considers the PPS of the WUFDSF properly design, operated and maintained and consistent with NSS No.13.

TRANSPORT REVIEW (MODULE 3)

XII. PHYSICAL PROTECTION MEASURES FOR NUCLEAR MATERIAL DURING TRANSPORT

In garnering a view on Module 3 as part of this IPPAS Mission, the Team was offered limited exposure to the processes, procedures and transport security standards operating at the national level. Accordingly, the majority of analysis and subsequent judgements regarding transport security in Canada stem from the Team's experiences during discussions and a visit to the Western Used Fuel Dry Storage Facility (WUFDSF) (situated within the Bruce Power site).

On this basis, it is inappropriate for the report to adhere to the standard formatting of a Module 3 assessment and therefore, rather than deliver substantial duplication across the document, much of the details (where not directly related to the movement of nuclear materials) are present only in Module 2 (Facility Review).

The IPPAS team considers that Canada has a strong regulatory mechanism and that CNSC provides a clear and consistent set of comprehensive security measures during transport of nuclear material.

XII.1. Transport Security Legislation and Regulations

In Canada, specific requirements for the transportation of Category I, II or III Nuclear Materials are enshrined within Section 5 of the NSRs (Nuclear Security Regulations). That secondary legislation specifies that licensees must apply for a licence to transport Category I, II or III nuclear material which shall contain, inter alia a written transportation security plan. The plan must incorporate details on:

a. the name, quantity, radiation level in Gy/h, chemical and physical characteristics and isotopic composition of the nuclear material;
b. a threat assessment consisting of an evaluation of the nature, likelihood and consequences of acts or events that may place prescribed information or nuclear material at risk;
c. a description of the conveyance;
d. the proposed security measures;
e. the communication arrangements made among the licensee, the operator of the land vehicle transporting the nuclear material, the recipient of the material and any off-site response force along the route;
f. the arrangements made between the licensee and any off-site response force along the route;
g. the planned route; and
h. the alternate route to be used in case of an emergency.

A regulatory guide, G-208, *Transportation Security Plans for Category I, II or III Nuclear Material* offers assistance to licensees in the formulation of a written security plan.

The transport of nuclear substances in Canada is a regulated activity and licensees are involved in the majority of shipments. The CNSC issues licences and certificates for certain kinds of packaging and transportation of nuclear substances as stipulated in the *Packaging and Transport of Nuclear Substances Regulations 2015.* These regulations are based on the IAEA's *Regulations for the Safe Transport of Radioactive Material, 2012 Edition*.

The licenses and certificates include:

a. Licence to transport Category I, II or III nuclear material
b. Licence to transport nuclear substances while in transit
c. Licence to transport nuclear substances contained in large objects
d. Licence to transport nuclear substances when the transport cannot meet all the regulatory requirements
e. Licence to transport nuclear substances which require a multilateral approval of shipments
f. Licence to transport nuclear substances which require a special use vehicle
g. Certificates for the design of packages and special form radioactive material

The most recent Annual Report prepared by the CNSC confirms that (during 2013-2014), the Commission issued 163 new transport licences, revised 66 transport licences.

Additionally, the IPPAS team understands that the role of Transport Canada with respect to the nuclear sector is to promote public safety during the transportation of dangerous goods. Accordingly, the Transportation of Dangerous Goods Directorate is the leading source of regulation, information and advice on dangerous goods transport for the public, industry and government employees.

State responsibilities relating to the transportation of dangerous goods are covered under the Transportation of Dangerous Goods Act and an arrangement (MoU) between CSNC and Transport Canada confirms Transport Canada's responsibilities as follows:

a. regulating the handling, offering for transport, transport and import of dangerous goods (pursuant to the Transportation of Dangerous Goods Act, nuclear substances, within the meaning of the NSCA, that are radioactive, fall within class 7 of dangerous goods);
b. providing consultations to CNSC, which is responsible for regulating all aspects of physical security of nuclear substances and prescribed equipment, as defined under NSCA and its regulations, with regard to such regulation;
c. consultation on other issues related to Class 7 Dangerous Goods.

Additionally, an Emergency Response Assistance Plan (ERAP), approved by Transport Canada, must also be in place before the issue of any licence in cases where the relevant nuclear material is classified as fissile. The IPPAS team understands that Canada undertakes a variety of nuclear material transfers and transports annually.

The IPPAS team was assured that the principles and specificity of this legislation provided sufficient clarity for both the CNSC and licensee to ensure delivery of comprehensive levels of security compliance.

XII.2. Transport Security Management

During the IPPAS team's visit to the Western Used Fuel Dry Storage Facility (WUFDSF) (situated within the Bruce Power site). WUFDSF discussed transport security and showed the IPPAS team a video demonstration of a Category II transport which moved nuclear material from the Bruce Power reactor to the Dry Storage Facility (on site).

During engagements with the CNSC and representatives of the OPG WUFDSF, the IPPAS team gained assurance that management and oversight of the transportation process was robust and competent. Indeed, there was assurance that the OPG team at the WUFDSF operates a network of complementary elements which include: management and focus on nuclear security governance, planning, security operations, administration and capital improvements.

OPG's security programme is implemented through a program of Standards, Procedures and Instructions and the IPPAS team was advised that OPG regularly communicates the requirements for procedural use and adherence and assures compliance through observation, coaching and internal audit programs.

XII.2.1. Threat and Target Identification

Analysis of the threat and associated target identification for transportation of nuclear materials does not vary from the processes utilised elsewhere within the Canadian civil nuclear and regulatory framework. Accordingly, during the visit to the OPG WUFDSF, the IPPAS team was able to confirm that OPG work with a variety of Canadian national agencies including CNSC, Public Safety Canada, CSIS, the RCMP, local and provincial law enforcement in order to ensure relevant threats can be analysed and appropriate action plans developed.

XII.2.2. Allocation of Responsibilities

During the IPPAS team's visit, it was able to gain an insight into the allocation of responsibilities within the regulatory and oversight regime. This included confirmation that, the responsibility for inspections of transportation activities falls to the CNSC Security Division.

Additionally, the OPG Security and Emergency Services, programs division maintains an accountable manager who provides oversight for the security program at Nuclear Waste Management Facilities, including WUFDSF. These accountabilities for security services at WUFDSF are documented in a Service Level Agreement between Bruce Power and OPG and the program is monitored through regular communication, quarterly interface meetings and formal and informal self- assessments.

OPG's Performance Improvement division (Internal Audit) conducts reviews of OPG's security program, including the interface with Bruce Power.

XII.2.3. Transport Security Plan, including Contingency Plan

In accordance with NSS No. 13, prior to commencing the transport operation, the carrier should always ensure all physical protection measures are in place in accordance with the transport security plan. During the IPPAS team's visit to the WUFDSF, it was able to confirm that transport security plans are always required by the CNSC for such movements.

XII.2.4. Interfaces with Safety and Nuclear Material Accountancy and Control

During the visit to WUFDSF, the IPPAS team was able to confirm the OPG maintains a Nuclear Material Accountancy System (NMAS). To ensure accuracy of the confidentiality, integrity and availability of the information, NMAS is incorporated within the licensee's cyber security programme. Additionally, security personnel are present whenever there is an on-site movement of the nuclear material.

Before the transportation (onsite movement) occurs, the Nuclear Security Officers inspect the DSC visually and then seal the container. The transportations of empty and full DSCs are escorted by the NRT (Nuclear Response Team).

XII.2.5. Security Staff Training and Qualifications

Refer to Module 2.

XII.2.6. Security Culture

Refer to Module 2.

XII.2.7. Confidentiality

Refer to Module 2

XII.2.8. Trustworthiness

Refer to Module 2.

XII.2.9. Reporting

The NSCA (Nuclear Safety and Control Act) requires that every licensee and every prescribed person shall:

a. keep the prescribed records….; and

b. make the prescribed reports and file them in the prescribed manner, including a report on (i) any theft or loss of a nuclear substance, prescribed equipment or prescribed information that is used in carrying on any activity that is authorized by this Act, and (ii) any contravention of this Act in relation to an activity that is authorized by this Act and any measure that has been taken in respect of the contravention.

Additionally, the GNSCR s29.1 requires that licensees immediately provide a preliminary report to the Commission of the location and circumstances of security related events including but not limited to sabotage, breach of security and of any action that the licensee has taken or proposes to take. Further, any changes to the licensee site security program must be reported in accordance with the licensing.

For the purposes of transport security, the IPPAS team was able to confirm that there are established requirements to report security events. Specifically, in these cases, the consignor, carrier and consignee must report to CNSC any 'dangerous occurrences'. They include vehicle accidents, damage, loss or theft to packages and contamination of packages.
Preliminary reports must be made 'immediately' and subsequent reports must be made within twenty-one days.

XII.2.10. System Evaluation, including Performance Testing

During the IPPAS team's visit to the WUFDSF, it was confirmed that security at the entire site is delivered by Bruce Power. Bruce Power Security has an extensive training program for its Nuclear Security Officers and conducts regular drills and exercises at its facilities and has contingency plans in place to respond to events within the Bruce Site, including WUFDSF. Bruce Power also conducts a number of Drills specifically at WUFDSF and all drill reports are reviewed by the OPG SES Programmes to ensure regulatory requirements are achieved.

The Performance Testing Program (PTP) includes force-on-force exercises conducted (at a minimum) every two years and joint exercises with off-site response forces are also undertaken. Notwithstanding this extensive testing programme, the IPPAS team failed to gain assurance that exercises (on or off site) which had a specific transport security focus, were delivered with any regularity.

Suggestion: To accord with sound international good practice, CNSC should encourage the development of regular transport security exercises incorporating Design Basis Threat scenarios including on and off-site response forces.

XII.2.11. Quality Assurance

Refer to Module 2.

XII.2.12. Sustainability Programme

Refer to Module 2.

XII.3. Transport Physical Protection System

The IPPAS team's exposure to transport security processes within the Canadian nuclear program focused on the activities at the WUFDSF. WUFDSF comprises a processing building and four storage buildings. It maintains a staff of 39 and process over 100 Dry Storage Containers (DSCs) annually. WUFDSF processes and stores used fuel from Bruce A and Bruce B Generating Stations.

The majority of nuclear material moves within the Bruce Power owner controlled area, and are considered Category II movements.

In such cases, these transports are considered as Category III Nuclear Material. OPG submits an annual Transportation Security Plan to the CNSC with respect to these shipments.

As part of the Category II transport process, fuel from the wet bays is loaded at the stations into DSCs and transported to WUFDSF where the container is processed (sealed) and placed into storage. After the container is welded, closed and inspected, the IAEA attends the site and attaches seals to the containers which are then placed into storage.

Category II used fuel is transferred from the station wet bays in DSCs equipped with a transfer clamp, and under security escort. These transfers remain within the site controlled area. A Transportation Security Plan for these on-site transfers is included in the Site Security Report for the WUFDSF and reports are submitted to the CNSC for acceptance.

During the movement process, a 'special purpose' built DSC transfer vehicle is used for transport between Bruce NGS and WUFDSF as shown in Figure 24. The DSC is loaded onto the vehicle deck and off-loaded using a crane which is controlled

Figure 24. A DSC Transfer Vehicle

The self-loading Liftking transporter vehicle (see Figure 25) is primarily used for moving DSCs within WUFDSF. It may also be used for transfers whilst inside the WUFDSF, the vehicle speed is limited to five kilometers per hour. It is not often used for transfers between sites due to its low speed.

Figure 25. Liftking transport vehicle

Liftking will be replaced with the GEN4 DSC Transporter Vehicle. GEN4 which can operate to speeds of twelve km/hr, has an onboard vehicle health monitoring system and can operate via remote control. It has five kill hardwired switches, one at each corner of the vehicle and one inside the cab.

Good practice: The use of kill switches in vehicles used for the transportation of DSCs is a good practice.

Notifications of planned transports take place between the licensee and the Regulator through encrypted and secured means.

XII.3.1. Detection

At the WUFDSF (and during associated on site transportation of Category II nuclear materials, security staffing is provided by Bruce Power Security under The Bruce Site Services Agreement.
During movements of the nuclear material, Bruce Power Security patrols with mobile surveillance capabilities provide 24/7 response to alarms or events at the WUFDSF. Bruce Power Security also conducts random regular patrols around the exterior of the facility.

XII.3.2. Delay

During the visit to the WUFDSF, the IPPAS team was able to establish understanding of the delay measures associated with the transport of nuclear materials between Bruce Power and the WUFDSF.
Delay is achieved principally through the robust nature of the DSCs (see Figure 26) used for the transfer of the relevant material. The DSCs are very robust containers. Their walls are constructed in 0.52 m reinforced concrete with a 1.3 cm outer and inner steel liner. Lids weigh five metric tons and are welded in place. The overall weight of a DSC is approximately 70 metric tons when full. DSCs are never left without a lid.

During transportation, the DSC lid is always secured to the base by a transfer clamp. The transfer clamp is designed to prevent the lid from separating from the base during design basis accident conditions.

At the site, in anticipation of disruption to transports from Design Basis threats, delay measures are similarly comprehensive. The perimeter is surrounded by interconnected concrete Jersey Barriers which provide protection against forced vehicle penetration by a design basis threat vehicle. There is an active vehicle denial barrier at the vehicle entrance. The vehicle entrance also contains a vehicle search portal that isolates the vehicle during search.

Figure 26. Dry storage containers

XII.3.3. Response

Refer to Module 2.

SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4)

XIII. NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL

XIII.1. Assignment of Nuclear Security Responsibilities

XIII.1.1. State

Canada has provided political commitment to both the IAEA Code of Conduct on the Safety and Security of Radioactive Sources and the Guidance on the Import and Export of Radioactive Sources.

XIII.1.2. Regulatory body

The CNSC's mandate covers regulation of facilities and activities related to nuclear materials and radioactive materials.

Under authority of the NSCA, the CNSC also functions as the authority for the development of regulations and is authorized to issue regulatory documents, issue relevant licences (e.g. licencing of possession, transfer, import, export, use and abandonment of nuclear substances), inspect activities and apply enforcement measures with the respect to radioactive material.

Pursuant to the Transportation of Dangerous Goods Act and according to the Memorandum of Understanding between Transport Canada (Transport Dangerous Goods Directorate) and the CNSC, Transport Canada is responsible for regulating the handling, offering for transport and transport of dangerous goods, including Class 7. Pursuant to the Transportation of Dangerous Goods Act, nuclear substances, within the meaning of the NSCA, that are radioactive, fall within Class 7 of dangerous goods.

The IPPAS team was informed that other governmental agencies authorities also have functions related to the security of radioactive material. However, these functions are designated in the same manner as described under section II.1.2 (Executive branch) of the report (i.e. they are not prescriptively described in the respective Acts of their establishment, but rather fall under their general mandate).

XIII.1.3. Operator, Shipper and/or Carrier

Section 12(1) of the General Nuclear Safety and Control Regulations describes obligations of the licensees. For the purpose of the General Nuclear Safety and Control Regulations, licensees are described as "a person who is licensed to carry on an activity described in any of paragraphs 26(a) to (f) of the NSCA" (which includes carrying out activities such as to possess, transfer, import, export, use or abandon a nuclear substance and to produce, process, package, transport, manage, store or dispose of a nuclear substance).

Respectively pursuant to section 12(1) of the General Nuclear Safety and Control Regulations the licensees are obligated to:
1) maintain the security off all nuclear facilities and nuclear substances (section 12(1.c));

2) implement measures for alerting the licensee to the illegal use or removal of a nuclear substance (section 12(1.g));

3) implement measures for alerting the licensee to acts of sabotage or attempted sabotage anywhere at the site of the licensed activity (section 12(1.h));

4) instruct the workers on the physical security program at the site of the licensed activity and on their obligations under that program (section 12(1.j).

The aforementioned means that responsibility for security of nuclear substances is vested in the licensee.

XIII.2. Legislative and Regulatory Framework

As the purpose of the NSCA is to provide for the limitation, to a reasonable level and in a manner consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information (section 3(a) of the NSCA), the NSCA must be considered the principal legal instrument for establishing requirements related to radioactive material. The aforementioned may be declared as pursuant to respective paragraph of section 2 of the NSCA, the concept "nuclear substances" includes radioactive material, however, in the opinion of the IPPAS team, that may cause confusion while implementing regulatory requirements and may imply possible inconsistencies with the IAEA's and internationally used terminology where most radioactive material is not labelled under "nuclear".

For more on the scope of the NSCA, see section III.2.1 of the report ("Nuclear Safety and Control Act (NSCA)").

Secondary legislation requirements related to security of radioactive material are stipulated in the following regulations: General Nuclear Security and Control Regulations, Radiation Protection Regulations, Nuclear Security Regulations, Packing and Transport of Nuclear Substances Regulations, Class II Nuclear Facilities and Prescribed Equipment Regulations, Nuclear Substances and Radiation Devices Regulations. For more on the scope of the documents mentioned above, see III.2.2 of this report ("Regulations").

There are also regulatory documents related to the security of radioactive material. For example, REGDOC 2.12.3 *Security of Nuclear Substances: Sealed Sources*, that apply in respect to implementation of security requirements for category 1, 2 and 3 radioactive sealed sources and provision of security guidance for category 4 and 5 radioactive sealed sources, which include minimum security measures which licensees must implement to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of sealed sources during their entire lifecycle, including while they are in storage, transport or being stored during transportation.

XIII.3. International Cooperation and Assistance

According to the information provided to the IPPAS team, the Government of Canada is expected, by international conventions (see below), to notify international partners in the event of a nuclear emergency that affects public health or that may have radiological impacts beyond Canadian borders.

Concerning specifically para. 12 of the IAEA Code of Conduct and para 3.16 of NSS 14, CNSC's Nuclear Security Division has the responsibility for the IAEA's Incident and Trafficking Database (ITDB). There are also MoUs with the regulators of neighbouring countries, e.g. US Nuclear Regulatory Commission, through which the information connected to the loss and control over

radioactive sources or incidents with potential transboundary effects involving radioactive sources is provided.

Additionally, according to information provided to the IPPAS team, detailed information on loss and control over radioactive sources is provided within 3 days on the CNCS's web site (Lost and Stolen Sources), e.g. the number of the device, which as an open source could be used by other governmental bodies, e.g. the police. Also, according to the provided information, when a sealed source is reported lost or stolen, a notification is sent to all interested third parties, such as metal recycling associations. The CNSC also uses an internal database to track outstanding issues, the Regulatory Information Bank (RIB) and Event Information and Tracking System (EITS) where such events would also be recorded and tracked.

XIII.4. Identification and Assessment of Threats

In Canada, the Threat Assessment incorporates classified, all-source intelligence from Government stakeholders engaged in intelligence and security. Those stakeholders include (principally, but not exclusively), the Canadian Intelligence and Security Service (CSIS), the RCMP and the ITAC. Additionally, the IPPAS team received assurances that contributions to the Threat Assessment, utilising sensitive intelligence, are garnered from a variety of valuable international strategic security partnerships to which Canada subscribes. For more analysis on the Threat Assessment and the DBT, see Module I, Chapter V.

For Nuclear Material there is both a Threat Assessment and a Design Basis Threat. However, for Radioactive Material the Competent Authority decided that a nationwide Threat Assessment would be most appropriate. This accords with the recommendations in NSS No. 14 and NSS No. 11.

Following the national Threat Assessment, the CNSC recommends that licensees develop and maintain a site specific threat and risk assessment to determine vulnerabilities in the existing physical protection systems designed to protect against the loss, sabotage, illegal use, illegal possession, or illegal removal during the storage or transportation of sealed sources. This could include:

- identification of assets that require protection
- credible threats
- mitigation measures to minimize any identified threats, risks or vulnerabilities

The CNSC recommends that the licensees review and update the threat and risk assessment annually or as required, based on changes that affect the threat level.

The security requirements placed upon the licensee must be commensurate with the categorization, threat level and/or level of risk set by the licensee or the Government of Canada.

The IPPAS team believes that the CNSC is fully compliant with the recommendations in NSS14 regarding *Identification and Assessment of Threats*, and with the those on *Threat Assessment*.

As for communication of punctual threat information, the Competent Authorities have a well structured network established and are able to quickly inform licensees about emerging threats. On top of that, most licensees have a very good relationship, often documented in MoUs, with local authorities who can also keep the licensees informed about potential local threats. As these practices are common for all Nuclear Substances, more analysis about this can be found in chapter V.

XIII.5. Risk Based Nuclear Security Systems and Measures

At the national level the CNSC has invested considerable effort in a National Sealed Source Registry (NSSR) and Sealed Source Tracking System (SSTS). All high-risk (category 1 and 2) radioactive

sources are tracked and all five categories of radioactive sources are recorded in the National Sealed Source Registry. The NSSR contains detailed information on high-risk sources, and some information on moderate (category 3) and low-risk sources (categories 4 and 5). This system, in conjunction with regulatory licensing and compliance operations, increases both the safety and the security of those sources.

Good Practice: The fact that the CNSC registers all five categories of sources in a national database, together with the level of detail of the information that is stored, is a good practice.

The provisions in the regulation are based on the national threat assessment for sealed radioactive sources.

The regulation recommend that the operator take into account their security system, the national threat assessment and the site specific threat and risk assessment for their facility. Both the facility threat assessment and the way the security system addresses the threat, are reviewed by the CNSC.

- The legislative and regulatory framework takes into account the potential threats, potential consequences and likelihood of malicious acts on a national level, and requires the licensee to do the same on a facility level
- The CNSC requires, through the security systems of the operators and based on their Threat and Risk Assessment, the reduction of the risk associated with radioactive material. The CNSC itself takes some steps as well towards reducing the risk associated with radioactive material, for example through special projects for increasing device delay and quick disposal of disused high risk radioactive sources.
- REGDOC-2.12.3 Security of Nuclear Substances: Sealed Sources uses the graded approach and categorization of radioactive material and the concept of defence in depth, including a mixture of hardware, procedure and facility design.
- Regarding the establishment of security levels, the regulation takes into account both the D-values and the specific use-types, based on the NSS11 approach. It also accounts for aggregation, which makes the security levels even more conservative.

XIII.5.1. Risk Management

The requirements use a graded approach, taking into account the IAEA categorisation for radioactive sources. Additionally the requirements are risk informed and take into account the national Threat Assessment for racioactive sources. The requirements also oblige the licensee to take into account its own Threat and Risk Assessment).

REGDOC-2.12.3 requires security provisions for the prevention of both theft and sabotage (as well as loss, illegal use, illegal possession and illegal removal) of radioactive sources. The focus of the licensee however, will mostly depend on their own Threat and Risk Assessment. The IPPAS team was also able to observe this at the visited facilities.

XIII.5.2. Interface with the Safety System

NSS No. 14, para 3.25 "…the State should ensure that:… Consultation and coordination are maintained between those responsible for safety and security to ensure efficient security of radioactive material…Major decisions regarding safety and security require participation of experts in safety and in security on a continual basis…".

CNSC safety and security inspectors/experts work closely together and (as a result of the substantial efforts invested in creating joint working practices), the formalisation of inspection arrangements between the two specialisations works well. The overwhelming majority of sealed source security

compliance verifications are conducted by suitably trained safety inspectors (with support from NSD security inspectors). This cooperation is documented in the Protocol between the Directorate of Nuclear Substance Regulation and the Directorate of Security and Safeguards Regarding Security Inspections of DNSR Licensees. As a result of this arrangement, the IPPAS team is confident that potential concerns regarding safety-security interface could be identified rapidly. The IPPAS team believes that the effort the CNSC put in the cooperation between "*those responsible for safety and security*" has led to a strong synergy between these two disciplines.

REGDOC-2.12.3 requires that licensees' general security measures (3.1) "*shall integrate safety and security concepts involving industrial safety arrangements, radiation protection measures and appropriate design to achieve the necessary level of protection against unauthorized removal of radioactive sources.*"

To further enhance the benefits CNSC has derived from its cooperation between its nuclear safety and nuclear security areas, the CNSC could provide guidance to licencees to promote consultation and coordination between those responsible for safety and security, where applicable.

XIII.6. Sustaining the Nuclear Security Regime

According to IAEA NSS No.14 (para 3.29), "*the State should commit the necessary resources, including human and financial resources, to ensure that its nuclear security regime is sustained and effective in the long term to provide adequate nuclear security for radioactive material*."

Although the regulation for the security of radioactive material is a relatively young, it is mature. The specific threat is clearly identified, the system is graded and risk based, and all the required topics are addressed in the regulation. Most security topics are covered during safety inspections and there are established protocols and processes in place to have security inspectors/experts go more into detail when needed.

NSS No. 14 mentions that the foundation of a nuclear security culture should be the recognition that 1) a credible threat exists, 2) that preserving nuclear security is important, and that 3) the role of the individual is important. All those three aspects are clearly present in the CNSC approach. The Nuclear Security Division invested in reaching out to other divisions within the CNSC, particularly to the safety inspectors, and to the sector, and raised awareness for and understanding of the security of radioactive sources. The different outreach activities such as presentations, articles, information on the website, clearly illustrate this.

The CNSC invests great effort in order to assure that its (safety) experts and inspectors are properly trained in the field of nuclear security. The training, awareness and refresher program appears to be solid. The number of dedicated security personnel at CNSC however, is in contrast with this approach. For specific security inspections at licensees with high-risk radioactive sources, there are currently a limited number of dedicated security inspectors for the whole country. The IPPAS team was informed that two additionnal security inspectors are currently being hired and trained.

Apart from the security inspections performed by the safety inspectors, the CNSC also appoints dedicated security experts to perform certain security inspections. The NSD has a program to inspect every facility with high-risk radioactive sources at least once every five years based on a risk-informed basis. Also, the security inspectors perform frequent and *ad hoc* inspections in facilities with significant threat levels , or in facilities where safety inspectors identify security issues. Taking into account the high number of risk significant sealed sources in Canada and the wide geographic distribution of regulated entities, the IPPAS team considers this a challenging objective with the

current number of dedicated security inspectors. This concern is also addressed in the recommendation in Module I, Paragraph IV.2.

XIII.7. Planning and Preparedness for and Response to Nuclear Security Events

The CNSC requires licensees to have and implement emergency preparedness programs and infrastructure commensurate with the level of risk of the facility or activity. The CNSC reviews them as part of the licensing process and their implementation is reviewed through ongoing compliance inspections and audits. The licensee programs include provisions to locate and recover missing or stolen nuclear substances.

On a governmental level, Public Safety Canada coordinates departments and agencies responsible for national security. The necessary plans on local, provincial/territorial and national levels are in place. MoUs exist between the licensee and responders.

XIII.7.1. Trustworthiness

Licensees in posession of high-risk radioactive sources, have to verify the trustworthiness and reliability of all persons who require access to sealed sources at the licensee's location or to prescribed/sensitive information, including servicing companies, contractors and building maintenance staff who require access without escort. Personnel who require access to such radioactive material or prescribed/sensitive information to perform job duties, but who are not approved by the licensee, must be escorted by an approved individual. The licensee has to base the nature and depth of personnel screening on the category of the radioactive material.

In REGDOC-2.12.3, the CNSC sets out minimum information that needs to be verified and states that trustworthiness and reliability verification shall be updated on a regular basis; at a minimum, every five years. The licensee has to document its trustworthiness and reliability process and allow the CNSC access to the corresponding records.

XIII.7.2. Reporting

Reporting nuclear security events is not addressed in REGDOC-2-12-3 because it is not specific to sealed sources. General provisions are present in "General Nuclear Safety and Control Regulations, SOR/2000-202" NSRDR 38 requires reporting of lost and stolen substances.

In this document the CNSC requires the licensee to report certain security event related information immediately, as well as providing a full report of the situation within 21 days after becoming aware of the event. The list of events to be reported contains amongst other any attempted or actual breach of security or any attempted or actual act of sabotage at the site of the licensed activity.

XIII.8. Import and Export of Radioactive Material

In accordance with requirements defined in the Nuclear Non-Proliferation Import and Export Control Regulations, 492 export licenses and 157 import licenses were issued in fiscal year 2014/15 for nuclear substances, prescribed equipment and prescribed information. An additional 212 export licenses were issued in the same time period for risk-significant radioactive sources, in accordance with the General Nuclear Safety and Control Regulations.

Canada is an important worldwide exporter of radioactive sources, as well as a substantial importer. Canada consistently applies the Guidance on Import and Export of Radioactive Sources and strongly encourages her trade partners to do the same.

Guidance on the Import and Export of Radioactive Sources, para 21:

States should, as necessary and appropriate, exchange relevant information and consult with other States.

In order to facilitate this exchange of information and consultation, the CNSC encourages its trade partners to establish Administrative Arrangements for the import and export of radioactive sealed sources between the two States. At this moment the CNSC has established 12 such arrangements. This practice is to be encouraged.

Guidance on the Import and Export of Radioactive Sources, para 8: Evaluation of Request

"In deciding whether to authorize an export of such a source the exporting State should..."
The Guidance provides an extensive list of criteria, to be taken into account during the evaluation of an export request. These criteria also include security related topics, to be considered based upon available information. As such information is not usually readily available, not all States go through the same level of effort in trying to collect and consider this information. It should be noted that the CNSC uses an extensive checklist for these issues, uses a risk informed approach and applies a detailed and conservative evaluation. Some of the aspects they evaluate go beyond what the Guidance prescribes. Figure 27 shows an extract from an Export Evaluation Form.

Good practice: The risk informed and systematic approach, and the level of detail in which the CNSC applies in evaluating requests for export can be considered a good practice. Particular attention is given to the end-use and end-user, safety and security, the importing state, the final and the intermediate consignee, as well as other information from open sources, domestic and foreign watch lists.

SECTION 5 - FINAL CONSIGNEE ASSSESSMENT:

5.1 Is this a new facility/operation? No

5.2 Indicate the number of years facility has been in operation?

5.3 Does the End-User have an established business arrangement with the Exporter? Yes

5.3.1 If known, provide number of years Exporter has dealt with End-User:

5.4 Has the CNSC or another Exporting State previously denied receipt of nuclear substance to End-User? No

5.4.1 If Yes, provide details of denial:

5.5 Through open-source information, has the End-User been involved in any radiological incident? No

5.5.1 If Yes, provide details of denial:

5.6 Is the End-User listed on any Domestic or Foreign watch lists? No

5.6.1 If Yes, provide details below:

Figure 27. Extract from Export Evaluation Form

XIV. Nordion – Kanata, Ontario

Nordion is a health science company, exporting gamma technologies and medical isotopes all around the world. As the managers declared, Nordion is focused on providing a safe and healthy working environment for their employees, and is deeply committed to safety, quality, integrity and corporate social responsibility in everything they do. Nordion provides the following sterilization technologies:

- Gama sterilization is focused on disease prevention.
- Co-60 is used to sterilize single use disposable medical devices, instruments and supplies, tissue for transplant, artificial joints, endoscopic materials
- Customers of Co-60 include contract sterilization service providers and medical device and product manufactures.

The IPPAS team received a presentation and was given a tour of the facility, focussed on the Co-60 sources, including the storage pool, transport docks and the security monitoring room. Transports conducted for Nordion were discussed but not visited/observed and will not be analysed in this part of the report.

XIV.1. Security Management and Security Planning

It was evident that adequate importance is given to the allocation of financial and human resources for security. Significant resources (>$1.7 million) have been provided for security upgrades over the last few years. The team was provided an overview of Nordion's security procedures, policies, records and plans for security which appeared well structured. Apart from Nordion's full-time security manager, an Executive Security Committee meets regularly which indicates the importance security receives within the organization of Nordion.

Nordion's corporate security program elements (see Figure 28) includes: Personnel security, Physical security, Information security, Transportation security, Emergency management, Business continuity planning, Awareness, Security compliance and investigations and Workplace violence.

Nordion's IT security reports to Corporate Security. Proper attention is given to computer security through different means such as Network Intrusion Detection, Corporate Anti-virus and locked desktop administrative functions.

Nordion gives a high importance to security, which is an explicit part of the company's vision. There are different ad hoc and recurrent initiatives to promote security, such as an annual security awareness week. Additionally Nordion confirmed that:

- The trustworthiness of individuals is verified, For most employees background checks go back five years, for some even ten years. Many employees get an additional background check in the USA. Another means to increase trustworthiness of individuals is through the managers, who receive supervisor behavioral observation training;
- Sensitive information is identified and properly protected;
- A CNSC accepted security and contingency plan is being implemented;
- A capability to manage security events is ensured. See Security System – Response below for more details;
- There is a security event reporting system in place.
- A mandatory security awareness training is in place for active shooter incidents

Good practice: Nordion's strong security management system, which includes an executive security committee and comprehensive security management program, is recognized as a good practice.

Figure 28. Nordion Corporate Security Program Elements

XIV.2. Security System

Nordion has a well-designed and recently upgraded security system with integrated measures to perform Deterrence, Detection, Delay, Response and Security Management which is summarised below and expanded in later sections.

Deterrence: Nordion actively invested in deterrence by upgrading their security patrol vehicles designed to intimidate loiterers.

Detection: Several different and independent detection systems are present externally and internally to the production facility. See XIV.1.4. Intrusion Detection for more details.

Delay: Nordion provides different levels of delay, both for adversaries on foot (fences, walls, etc.) and for vehicles (vehicle barriers, anti-ramming cable in fences). There is an early detection system surrounding some parts of the facility, in order to make the delay measures relevant. See XIV.1.8. Delay for more details.

Response: Nordion uses both on-site guards and off-site response personnel. There are several layers of off-site responders available with good capabilities in relatively close proximity. There are MoU's with these responders and they consider Nordion as a priority. See XIV.1.9 (Guards and Response Forces) for more details.

Security Management: See XIV.1.1. Security Management and Security Planning

XIV.3. Access Control

Two layers of access control, using Nordion issued badges, effectively restricts access to areas holding radioactive sources (actives areas) to authorized persons only. Visitors must be escorted at all times. For access to the SMR, biometry verification is also required. The pair of access controlled doors at the main personnel entry are :

Most of Nordion's administrative functions are done in the adjacent "RE Building" located well outside the main external perimeter and detection system. This has the benefit of limiting the access to the main operations facility to operations staff only.

Access for vehicles loading and returning sources is through a vehicle portal and inspection station including a robust vehicle barrier (see Figure 29). The outer gate is opened by and the inner vehicle barrier after it has been inspected etc. The vehicle inspection is done under CCTV surveillance at the SMR in the dedicated inspection area between two gates. Only pre-registered vehicles are allowed to enter.

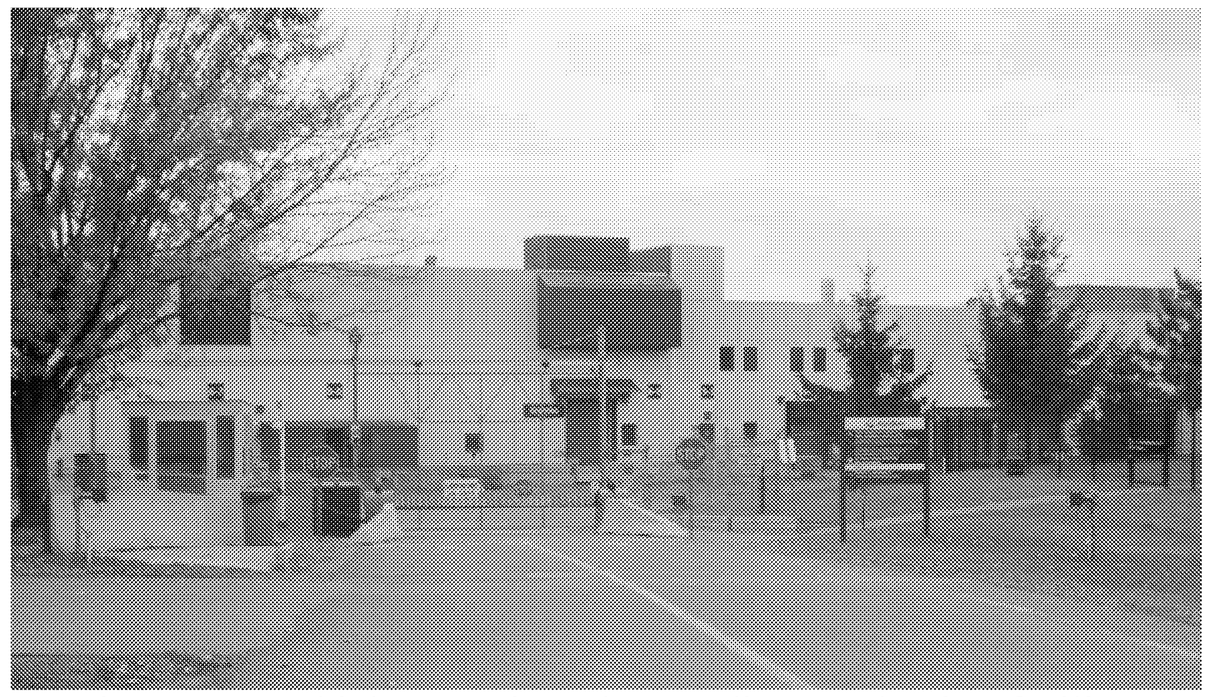

Figure 29. Vehicle entry into the Nordion production facility.

XIV.4. Intrusion Detection

Several different detection technologies and measures are present as part of the integrated detection system:

- Exterior detection sensors
- Video surveillance interior and exterior (including the roof) using over IP cameras which include a health monitoring capability.
- Patrol guards on duty 24/7
- Movement detection sensors inside the building
- Accountancy and control record for radioactive sources
- locks on personnel doors, shipment doors and roof hatches

When swiping the badge at the entry of the facility, a picture of the badge-holder will be displayed in order to detect attempts of intrusion with a stolen badge.

Contraband detection is done by checks for incoming transport vehicles under surveillance of the SMR,

For detection of unauthorised activities by insiders there is a heavy reliance on radiation alarms raising an alert in addition to CCTV surveillance and observation by other Nordion staff.

XIV.5. Alarm Assessment

Nordion has a local SMR in the production facility building with some monitoring features also available in the “RE Building”. On-site PTZ and fixed cameras are programmed to call on door openings and other detection events and automatically display on SMR monitors. Initial alarm assessment is done from the SMR from where the operator can coordinate further assessment and response with patrolling guards

to the SMR operator. During office hours operators are present in the SMR, and at night. Nordion trains as many of its guards as possible as SMR operators, which requires 80 hours on-the-job training before they are allowed to operate the SMR alone. Nordion plans to upgrade an

The IPPAS team visited the server room for the SMR which had

The IPPAS team was informed that the security network is not connected to the internet.

XIV.6. Emergency Power Supply

Nordion has an emergency power supply, covering the entire facility (including the physical security system) and with the capability to provide power for several days.

XIV.7. Locks and Keys

Keys are required to access specific locations but procedures for their use were not discussed.

XIV.8. Delay

Nordion provides different levels of delay against adversaries on foot (fences, walls, etc. and vehicles (vehicle barriers, anti-ramming cable in fences). There is an early detection system, in order to make the delay measures relevant. Delay times have been calculated through the use of Adversary Sequence Diagrams and other analyses. All external fire access doors to the licenced facility were upgraded to to increase resistance to attack. Additional barriers are placed in front of some of the external facing doors (see Figure 30 below).

Figure 30. Vehicle barrier in front of an external door

The IPPAS team noted that

Figure 31. Storage pool with Cobalt-60 sources

XIV.9. Guards and Response Forces

Nordion relies on both internal and external response personnel. Security personnel on-site are well trained, paid and equipped and there is little staff turnover. Guard on patrol check-in with the SMR Fourteen local police units routinely patrol in Nordion's vicinity. The proximity of Ottawa provides availability of many additional off-site responders, including those with CBRNE capabilities and skills. There are MoU's with these responders and they consider Nordion as a priority.

There is regulator cooperation and interaction among these responders.
Regular exercises, both announced and unannounced, ensure their guards stay focussed.
Nordion can also apply additional temporary security measures should the threat situation warrant this.

XIV.10. Communications and other Equipment

Personnel in the SMR have the necessary communication equipment to communicate with security management, guards on the site and offsite responders.

XIV.11. Contingency Plan

Nordion has a contingency plan, linked with their security plan in accordance with CNSC requirements.

XIV.12. Other Observations

It was observed that Nordion's security measures are above and beyond what is normally expected for a category 1 source licensee. Some of their measures are justified given their threat and risk analysis and very large inventories involved, but even then it is clear that Nordion is setting security arrangements at a high level. This is also reflected in the fact that they received a fully satisfactory security inspection report from the CNSC.

The IPPAS team was impressed that Nordion had achieved Tier Three Status in the US Customs-Trade Partnership Against Terrorism (C-TPAT) where only top 2% of member organizations achieve this status.

XV. SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT

During 2013-2014, the CNSC issued 163 new transport licenses, revised 66 transport licenses and issued 19 transport certificates for package design and for special-form radioactive material. CNSC also issued 31 new certificates and revised 65 certificates for radiation devices and other prescribed equipment in 2013-2014

XV.1. Transport Security Requirements and Regulations

The CNSC and Transport Canada are jointly designated competent authorities for Canada with respect to regulating the transportation of radioactive material, as per the International Atomic Energy Agency, *National Competent Authorities Responsible for Approvals and Authorizations in Respect of the Transport of Radioactive Material List*.

Transport Canada is the designated competent authority for Canada with respect to the programs and activities of intenational modal organizations, such as the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO).

An MoU is in place between Transport Canada and the CNSC which contains principles, understandings and arrangments for their cooperation. In particular the CNSC is responsible for regulating all aspects of physcial security of nuclear substances against sabotage or theft, and carries this out in consultation with Transport Canada. Transport Canada regulates from the perspective of class 7 Dangerous Goods.

Given that there are two different organisations sharing the responsibility for the regulation of radioactive materials during transport, special attention needs to be given in order to assure both these organisations complement each other, and can together guarantee security.The existing MoU is certainly a good step in this regard.

XV.2. Security Management and Transport Security Plan

The CNSC provides specific requirements for the security of radioactive material in transport, in REGDOC-2.12.3. The implementation of these requirements is the responsibility of the licensed consignor. The carrier has to submit his security plan to the consignor, who has to demonstrate to the CNSC that it verifies the security plans of its carriers.

As an example of CNSC requirements for transport security, for the transport of a Category 1 radioactive source, the vehicles have to be equipped with a vehicle tracking device which enables the vehicle to be recovered if stolen and a duress alarm or an equivalent device that is continuously monitored. The licensee, should operate the alarm monitoring station from where he can alert the response force.

XV.3. Implemented Detection, Delay and Response Measures

Based on REGDOC-2.12.3, licensees must implement requirements for security during the transport that include hardware security systems for physical protection system functions of “detection, delay and response”.

The licensee must ensure the carrier takes the appropriate security measures required to be implemented during transport. The following measures for detection, delay and response are required:

- Vehicule security
- Security measures for sealed sources during the transport
- Packages or containers that are robust enough
- Vehicle disabiling device to prevent unauthorized removal
- Intrusion detection system to detect unauthorized acces
- Regular testing and maintenance of the security system or device
- Minimum two physical barriers
- Efective access control measures to detect
- Efective means to detect and assess unauthorized access
- Response protocol in place with a local response force

The transport is monitored by licensee and by the carrier for the entire duration of the transport including outside of the country.

XV.4. International Transports

Based on CNSC Regulations, as long as material is within the borders of a country, it is subject to the regulatory regime of that country. When shipments are made out of Canada, the responsibility for physical protection begins and ends at the borders of the concerned countries. Accordingly, if the material is to be imported into Canada, or exported from Canada, the receiver, or the shipper, respectively, must obtain from the CNSC, before the shipment crosses the border, the appropriate licence.

REGDOC-2.12.3 reflects the security goals of United Nations specialized agencies and programs – including the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO) and other intergovernmental organizations such as the International Carriage by Rail – as they have taken similar steps to provide improved security in the transport of dangerous goods carried by sea, air and rail.

These organizations have developed various instruments, such as the International Maritime Dangerous Goods Code, and technical instructions for the safe (and secure) transport of dangerous goods by air.

The IPPAS team considers that Canada has a strong regulatory mechanism and that CNSC provides a clear and consistent set of comprehensive security measures for sealed sources during transport in its Packaging and Transport of Nuclear Substances Regulations.

XVI. MITIGATION AND RECOVERY OF NUCLEAR AND OTHER RADIOACTIVE MATERIALS

XVI.1. Location and Recovery of Missing/Stolen Material

CNSC has an orphan source strategy that is applied when orphaned sources are identified. Local police and RCMP resources are available to pursue the recovery of missing or stolen nuclear substances.

For operators, licensees are required under section 38 of the Nuclear Substance and Radiation Devices Regulations to report to CNSC if a nuclear substance is stolen and within 21 days provide a report describing actions to “reestablish normal operations” and under section 3(f) of the Nuclear Security Regulations to have a plan in place to assess and respond to breaches of security. Licensees are also

required to develop contingency and emergency plans, for which the CNSC ensures that such plans include provisions to locate and recover missing or stolen nuclear material. However there is no explicit requirement in CNSC regulations that contingency plans include measures and procedures to locate and recover nuclear material either alone or in cooperation with outside resources as implied by 4.52 & 4.60 of NSS No. 13.

Suggestion: The CNSC should consider making it explicit in the regulations that licensees' contingency plans should include measures to locate and recover any missing and stolen nuclear substances.

XVI.2. Measures to Mitigate/Minimize Radiological Consequences of Sabotage

The Government of Canada manages and coordinates all federal response activities to mitigate nuclear emergencies that could affect Canada. If called upon to respond to a nuclear emergency under the Federal Nuclear Emergency Plan (FNEP), the CNSC will fulfil its responsibilities identified in the FNEP in addition to its natural regulatory oversight responsibility.

XVII. COMPUTER SECURITY STATE LEVEL REVIEW

XVII.1. Legal and Regulatory Framework

The loss or compromise of computer based systems at nuclear facilities could have a serious impact on nuclear security, nuclear safety and operations. Accordingly, computer security must be a component of the state's regulatory framework and also of the facilities overall nuclear security program.

In order to address the increasing relevance of computer security at nuclear facilities, CNSC updated certain regulatory documents and license conditions handbooks of high risk facilities. In 2008, CNSC sent a Regulatory Position Statement to all Nuclear Power Plants (NPP) licensees, outlining computer security expectations based on IAEA drafts and US regulatory documents. Accordingly, the IPPAS team acknowledges that the CNSC has demonstrated that all NPPs' site-specific computer security programs are in place. The CNSC focused primarily on those systems relevant to nuclear safety, security and emergency preparedness and has not yet reviewed nuclear accountancy and auxiliary systems in any depth. However, systems used for nuclear material accountancy are explicitly listed in NSS No.13 *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* to be protected against compromise. Additionally, in the Safety and Control Area of the License Condition Handbook, computer security requirements have been added for those cases, when licenses will be renewed. Typically, this is performed every five years and therefore has been enforced for a subset of the high risk facilities. The last license renewal for those facilities is scheduled for 2017.

Basis: NSS No. 13 para 4.10 and 5.19. Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat.

Recommendation: CNSC should review the protection afforded to nuclear accountancy and control systems and, if required, enhance regulatory controls to protect them against compromise.

Canadian Standard Association (CSA) standard N290.7-14 *Cyber Security for Nuclear Power Plants and Small Reactor Facilities,* section 1, para. 1.2 item (e) addresses cyber security as at nuclear power plants and small reactor facilities for the computer systems and components related to safeguards.

In 2014, CNSC addressed the issue of computer based threats in the Canadian Design Basis Threat (DBT). Although computer based threats cannot be described and quantified as conventional physical threats, their inclusion in the DBT will benefit all licensees. Without knowledge of the content in the DBT, the IPPAS team assumes computer based threats have been covered to include the standard threat vectors, such as the potential for external, internal and 'blended' attacks. The CNSC also confirmed that their team remains deeply engaged in the IAEA-sponsored forum to develop a Cyber DBT and the IPPAS team encourages the continuation of this engagement in order to guarantee the adoption of IAEA best practice, potentially to include the number, strategies and tactics of potential adversaries and an understanding of potential tools, technologies and attack scenarios including 'blended' attacks.

Currently, regulatory oversight and focus on computer security at licensed facilities is based on the CNSC Regulatory Position Statement from 2008 which focuses on operating NPPs. For other nuclear installations or licensees, regulatory requirements are not yet fully in place. CNSC has announced two further steps for delivering the necessary assurances, including the implementation of requirements according to Canadian Standard Association (CSA) standard N290.7-14 *Cyber Security for Nuclear Power Plants and Small Reactor Facilities* and (when the License Condition Handbook is renewed), the integration of computer security requirements in the relevant security section.

The IPPAS team positively acknowledges CNSC's activities regarding the implementation of regulatory requirements on computer security. This process is still underway and, at present, the activities are focusing on high risk facilities and the most appropriate way of prioritizing outputs. The next step should be the expansion of regulatory activities to all other licensees in a graded approach which takes into account the potential maximum safety and security significance.

The current rate of development in the information technology sector is substantial – and accelerating. Accordingly, technological changes occur rapidly and within short periods of time. This means it is a challenge to ensure computer security and the implementation and maintenance of adequate countermeasures keep pace with such developments. Accordingly, the IPPAS team noted that there is a risk that the CNSC's strategy of integrating computer security requirements into License Condition Handbook renewals may leave the potential for delays in installation of adequate measures at installations which do not fall into the category of high risk establishments. Accordingly, the IPPAS team believes CNSC should consider prioritizing the final rollout of their computer security activities program, to incorporate clear definitions of roles and responsibilities for key personnel and associated procedural and technical measures.

Suggestion: The Regulatory Position Statement from 2008 articulates only that NPPs should satisfy regulatory expectations relating to the implementation of updated and effective computer security management processes. The principles outlined in the 2008 letter should also be extended to cover regulatory expectations for all licensees.

The CSA standard N290.7-14 was published in December 2014. This standard is intended to form a licensing basis for all nuclear power plants and small reactor facilities in Canada. The IPPAS team was advised that the key driver for development of this standard came principally from representatives of the operators (assisted by CNSC) and validated through consensus across the industry. This approach has ensured the development of a computer security program will be practicable and applicable.

The IPPAS team suggests that CNSC consider the introduction of a regulatory document to enhance and frame the regulatory expectations for the delivery of a sound and secure computer security regime across the Canadian civil nuclear industry. Any such REGDOC might reference, refine, update and enhance elements of the current CSA documents.

There are clear divergences between the standards enshrined within other industry-led or IAEA guidance documents for cyber security (ISO 27000 or IAEA NSS NO.17 *Computer Security at Nuclear Facilities)* and N290.7-14.

For example:

- N290.7-14 Chapter 6.2.1 shows that the classification scheme depends on the "vulnerability to cyber threats" as one of two important factors. In principle, the vulnerability of a computer component or a system is not known and can almost never be determined. Usually, most of the vulnerabilities are hidden and undetected due to weaknesses in programming. Consequently, the vulnerability status may vary day by day. On the assumption that insider threats also have to be covered (potentially to include an administrator with maximum privileges), the level of potential vulnerability has to be set to "1". Since probabilistic approaches will also not be applicable in the computer security methodology, maximum safety or security significance will be the only reliable variable in a classification scheme. Of course, certain attack vectors may be excluded on a basis of analyses, e.g. attacks via wireless communication, when such connectivity is impossible.
- N290.7-14 Chapter 1.2 includes auxiliary assets or systems, while N290.7 – 1.4 excludes so-called "business systems". In the business domains of nuclear facilities a large amount of

information is stored electronically. Although individual pieces of information may not be critical, the aggregation of such disparate details (e.g. construction plans, I&C functional diagrams, cabling documentation, personnel information, plant status information, or emergency procedures) could become a critical factor to support an attacker.

Finally, the loss of integrity of information (e.g. manipulation of working procedures or technical documentation) could also affect safety or security. Accordingly, IAEA NSS No.17 *Computer Security at Nuclear Facilities* explicitly recommends consideration should be given to the protection of computer systems that are not necessarily within the scope of plant equipment, but nevertheless have the potential to impact safety (e.g. working permit systems, engineering and maintenance systems, configuration management systems, and document management systems).

- N290.7-14 Chapter 5.1.4 defines the role of a "cyber security program specialist". NSS No.17 recommends that such personnel should be independent of the implementing departments. This concept is not covered within the CSA standard.
- N290.7-14 Chapter 8.1.5 and 8.1.6 extensively reduces the set of controls under certain conditions. This potentially will reduce the effectiveness of a defence-in-depth approach.
- N290.7-14 covers insider threats only as an element of the product lifecycle rather than considered as a significant threat vector specified within the DBT. Additionally, as an unclassified document, it may be a challenge to include the specifics of subsequent regulatory protections requirements within N290.7. Accordingly, it is appropriate that a classified REGDOC be produced to ensure allow suitable levels of protection can be applied to future regulatory requirements.
- N290.7-14 does not require the implementation of a zone model with graded protective principles and applies only a classification scheme formatted on three levels.

NSS No.17 clearly defines the relevance of a robust defence-in-depth approach to the assurances for computerized systems. Such an issue does not appear to be a major guiding principle in the CSA standard.

Suggestion: In principle, the coverage and scope of CSA N290.7-14 addresses requirements for robust computer security in nuclear installations. However, the IPPAS team believes it may not necessarily be comprehensive enough to deliver the standards of assurance which accord with evolving regulatory expectations. Accordingly, CNSC should perform a systematic review of the document and decide (potentially on the basis of the 'cyber' DBT and within their own regulatory framework), which modifications or extensions are appropriate.

Suggestion: Based on the defence-in-depth approach, the CNSC should consider codifying minimum standards of IT security practices and processes for non-operational systems and encourage their adoption by all licensees.

In REGDOC-3.1.1 *Reporting Requirements for Nuclear Power Plants,* the CNSC stipulates specific reporting requirements following computer based attacks against NPP systems critical for safety, security, emergency preparedness and systems used for nuclear material accountancy and control.

The IPPAS team believes that, both at the CNSC and at the licensee site

Computer attacks by insiders differ in important ways from conventional and physical insider attacks.

On systems with the highest risks for plant safety and security adequate measures should be implemented that addresses this risk.

Suggestion: CNSC's ongoing activities on risk evaluation and the further development of the DBT should address the relevance of computer related insider threats, due to special attack mechanisms and capabilities.

Any Canadian Government information, which could compromise the physical protection of nuclear material and nuclear facilities is protected through adherence to appropriate legislation for protecting information and applying appropriate clearances (Policy on Government Security, 2009 Treasury Board of Canada Secretariat), and through GNSCR sections 21 to 23 and Nuclear Security Regulations. The CNSC confirmed to the IPPAS team that computer and information security at nuclear facilities is a priority for ongoing regulatory attention and is also receiving attention within the CNSC corporate structure.

The IPPAS team was able to confirm that assurances relating to the 'need to know' principle applied equally for access rights to information technology, including the operation of the CNSC IT infrastructure, which is part of a centralized governmental institution "Shared Services Canada (SSC)". Although those services are already being operated by the SSC, a Service Level Agreement comprising all CNSC protective requirements on information and infrastructure have not yet been endorsed.

The IPPAS team was also able to confirm the existence of robust controls relating to access rights to those rooms containing IT equipment and the handling and use of encrypted mobile media. Additionally, the team was able to gain an understanding of the Canadian information classification scheme and CNSC's implementation and management of the "need to know principle", underpinned by a mandatory online security training program. These are exemplary practices which demonstrate the CNSC's increasingly mature awareness of the demands of managing a robust information security regime. Finally, the IPPAS team noted that CNSC employees have the ability to remotely access selected applications through an encrypted connection on both CNSC and personal devices. Notwithstanding the robust security controls for this process, the IPPAS team considers this practice represents a sub-optimal security arrangement and should be abandoned in favor of arrangements which require CNSC employees to use government furnished equipment (GFE).

Suggestion: CNSC should strengthen the protection of sensitive information through certification of a Service Level Agreement with its IT supplier. Additionally, CNSC should require that only GFE be used for CNSC-related work access.

At the tactical level within facilities, sensitive information is protected through the GNSCR sections 21-23. Licensees are required to submit a site security report, which includes measures to protect prescribed information.

XVII.2. Roles and Responsibilities of Competent Authority

CNSC allocates responsibility for computer security of their licensing and inspection program to their system engineering division. As most of a nuclear facility's computerized systems centre on

instrumentation and control, the delineation and division of regulatory responsibilities along these lines makes sense. The IPPAS team acknowledges that, through the utilisation of this structure, the CNSC are demonstrating an efficient interdisciplinary approach to share, compare and contrast know-how from different disciplines. The IPPAS team also believes this structure allows close collaboration and cooperation, across and between specialisations.

CNSC has one dedicated specialist as a computer security expert within its System Engineering Division. However, there is a small number of other specialists who possess a basic level of professional expertise in computer security. The IPPAS team believes this does not represent an adequate level of resourcing to satisfy the scale of the regulatory challenge. Accordingly, the competent authority should be substantially reinforced by subject matter experts rather than through a relatively simple educational upgrade to the standard security matrix operated by regulators.

Suggestion: The complexity and scope of the computer security programme requires that CSNC consider reinforcing of relevant human resources.

In 2008, CNSC sent a Regulatory Position Statement to all NPP licensees, outlining computer security expectations based on IAEA draft documents and US regulatory documents which was followed by a program of inspections and assessments at nuclear facilities. Following responses to the 2008 letter, CNSC performed high-level desktop reviews on NPP licensees' computer security program designs and their implementation. In 2015, Darlington NPP was subjected to a pilot computer security audit and September 2015 Bruce Power was advised that it would be subject to a CNSC computer security inspection, to take place in November the same year. In anticipation of the inspection, the operator was requested to provide a set of more than twenty-seven documents, including the cyber security plan, a complete list of cyber assets, a list of critical systems, cyber security training records, event/incident reports and list of members of the Bruce Cyber Security Working Group including sample meeting records.

The CNSC inspection team will consist of five inspectors, one of whom will be a computer security specialist and one a representative of the nuclear security division. CNSC also provided the IPPAS team a draft guidance document on periodic inspections for plants cyber security programs. The IPPAS team considers this document suitable to assist and perform inspections with focus on computer security.

CNSC undertakes regular information exchanges on matters of IT security with other Canadian authorities involved in computer security. For an example, the Canadian Cyber Incident Response Centre (CCIRC) supports both regulator and operator in regard to computer threat evaluation. CNSC, national intelligence assets and the CCIRC are members of a cross departmental working group which meets monthly to share information on current computer threats. CNSC makes efforts to inform and update CCIRC members on cyber-related developments in order that an understanding of the nature of current threats is widely disseminated across the civil nuclear industry. Notwithstanding the valuable nature of this capability, subscription to the CCIRC threat and vulnerability notification matrix by licensees is voluntary.

Good Practice: CNSC regularly undertakes a cross departmental information exchange on the development of computer based threats and vulnerabilities.

Suggestion: CNSC should consider establishing a requirement that licensees must subscribe to the CCIRC threat alert and information capability. Following receipt of an alert, licensees should be required to institute appropriate mitigating actions.

XVIII. COMPUTER SECURITY FACILITY LEVEL REVIEW

During the visit to Bruce Power, the IPPAS team was able to observe various aspects of computer security, although time constraints prevented any opportunity to visit server or computer administration rooms, or specific security related IT equipment. Accordingly, this analysis is based primarily on evidence gained from presentations and consultations. The team did not have an opportunity to undertake any technical computer security analysis at any of the other operational utilities which were visited.

In general, Bruce Power demonstrated a high level of computer security management and provided the IPPAS team with sufficient confidence that resourcing the challenges of IT security was being taken seriously. The company demonstrated a highly integrated and interdisciplinary approach and an overall high level of awareness and practiced computer security culture. Bruce Power informed the IPPAS team that based on the results of a continuously internal improvement analysis, computer security enhancements are planned. This will require substantial investment and such funding has already been endorsed.

To continue developing computer security capabilities and programmes, the Canadian Nuclear Operators and the CNSC have continued meeting as a national working group. The pace of change in IT-based technologies and an associated rapid evolution of IT threats remains a substantial challenge. Accordingly, the ongoing exchange of information within the "nuclear community" offers a powerful protective opportunity for users. The Regulator should be aware of the potential for inhibiting a free flow of dialogue in such a forum if it is represented.

Good practice: The new licensee-initiated formal working group engagements between Canadian civil nuclear licensees for the purposes of ensuring wide understanding of computer based threats, vulnerabilities and associated best practice, is a Good Practice.

XVIII.1. Computer Security at Bruce Power NPP

XVIII.1.1. Computer Security Policy

In 2008, CNSC initiated a Cyber Security Action, advising facilities to evaluate their cyber security programs. At that time, no standard existed (even IAEA's NSS No.17 was still in draft) and therefore Bruce Power decided to adapt and apply NERC-CIP (North American Electric Reliability Corporation Critical Infrastructure Protection cyber security standards). In 2012 staff from Bruce Power chaired the committee tasked with the development of CSA standard N290.7-14 *Cyber security for Nuclear Power Plants and Small Reactor Facilities*. The standard was issued in December 2014 and the implementation of adequate controls and requirements at facilities is still underway.

In accordance with NSS No.17, Bruce Power introduced a specific cyber security policy for the management of its computer security systems. This is a 'Corporate' level document and applies to the entire facility. The policy also addresses requirements of N290.7-14, including review, maintenance and interfaces with other programs.

The IPPAS team was able to confirm that Bruce Power has already designated certain roles with defined responsibilities for computer security. The Cyber Security Governance Committee oversees the organization and delivers assurances across functional groups including Engineering, Physical Security, Information Technology, Emergency Preparedness and Operations. The Committee works at the strategical level and facilitates information exchange between the individual heads of departments. At the operational level, Bruce Power operates a Cyber Security Working Group with representatives

from the same departments. This group meets every two weeks, facilitates the interdisciplinary exchange of all computer security relevant information, implements the computer security program and also interfaces with other stakeholders such as Training, Control Maintenance and Communications. The Working Group is coordinated and chaired by the IT Security Officer.

In accordance with the recommendations within NSS No.17, the IT Security Officer is responsible for the overall security management process. Bruce Power instituted this role through the employment of full time computer security specialist, supported by a team of dedicated and experienced analysts. Currently, the IT Security Officer is part of the IT department and reports to the CIO. This decision was concluded after an analysis of the responsibilities of the post. In principle this role should be highly independent from IT operations and the IPPAS team concluded that there was indeed sufficient separation between the IT Security Officer and the operational part of the IT department. The IT Security Officer reports to, and receives directions from, the Cyber Security Governance Committee.

Furthermore, the IPPAS team acknowledged the existence of a high degree of cooperation between the Cyber Security Working Group and other disciplines and departments. Relevant changes on systems now all have a 'Cyber Security' element to ensure all aspects of a system's lifecycle receive a security review by Cyber Security Specialists. During discussions with the licensee, the IPPAS team was able to confirm that meetings on IT security take place at the facility on a near daily basis.

XVIII.1.2. Asset Management

The IPPAS team was informed that a process for the identification and management of computer components is established at Bruce Power. The assets are controlled by the computer security group in an Excel table. Each asset is assigned to a responsible person who will ensure the compliance of the asset with the computer security requirements in accordance with the system's functional allocation. The asset list is approved annually by Cyber Security Governance Committee and notified to CNSC. The systems and nodes identified on the asset list accord with those deemed most vulnerable to DBT actors.

A review of Bruce Power's guidance document for identification and management of cyber assets confirmed that the classification of critical digital assets still focuses strongly on systems important to nuclear safety.

Furthermore, the Bruce Power Cyber Security Policy is recommended rather than mandatory for critical cyber components, with the exception of those with a certain nuclear safety importance. According to the requirements in NSS No.13, <u>all</u> computer systems used for physical protection should be protected against compromise.

Basis: NSS No.13 Paragraph 4.10 and 5.19. Computer based systems used for <u>physical protection</u>, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyberattack, manipulation or falsification) consistent with the threat assessment or design basis threat.

Recommendation: The licensee should adapt and extend all relevant documents and procedures to ensure all computer systems used for physical protection are classified as critical digital assets and therefore follow the appropriate computer security processes.

According to N290.7-14, systems within the scope of asset management are those which perform or impact functions of nuclear safety (including fire protection), security, emergency preparedness and

safeguard/accountancy.

NSS No.17 recommends that consideration should also be given to computer systems not necessarily within the scope of plant equipment, but nonetheless might impact safety.

Suggestion: Bruce Power should include auxiliary systems, which might indirectly impact safety or security in their asset management register.

XVIII.1.3. Physical Protection and Environmental Security

The IPPAS team was informed that critical cyber components are situated within secure areas and their installation accords with standard physical security requirements.

In terms of clearances and associated access-rights to sensitive computer locations, the licensee confirmed that contractors are not permitted unescorted access to cyber components unless security-cleared.

With regard to the mitigation of the insider threat, the licensee confirmed its commitment to the principles of the graded approach to security. Accordingly, the licensee stated they utilize segregation of higher sensitivity systems which are maintained within areas under additional access control constraints.

The IT cabinets are also locked.

IT administrative activities can only be performed within this room or at a restricted level in the SMR. Finally, the cable routes between the IT server room and the SMR are protected against manipulation and alarm protected.

XVIII.1.4. Computer Operations Management

Bruce Power operates a powerful centralized computer security monitoring station (see Figure 32) which collects relevant information from different networks and domains, including safety and security related systems. Critical software on systems is “fingerprinted” so that automated integrity checks are performed. In case of manipulation and loss of integrity, an alarm is given to a Computer Security Operations Centre. This approach assists early detection of anomalies or attempts at intrusion.

Good Practice: Bruce Power’s operation of a comprehensive centralized Computer Security Monitoring Center, which collects relevant information from different networks and domains assists early detection of anomalies or attempts of intrusion.

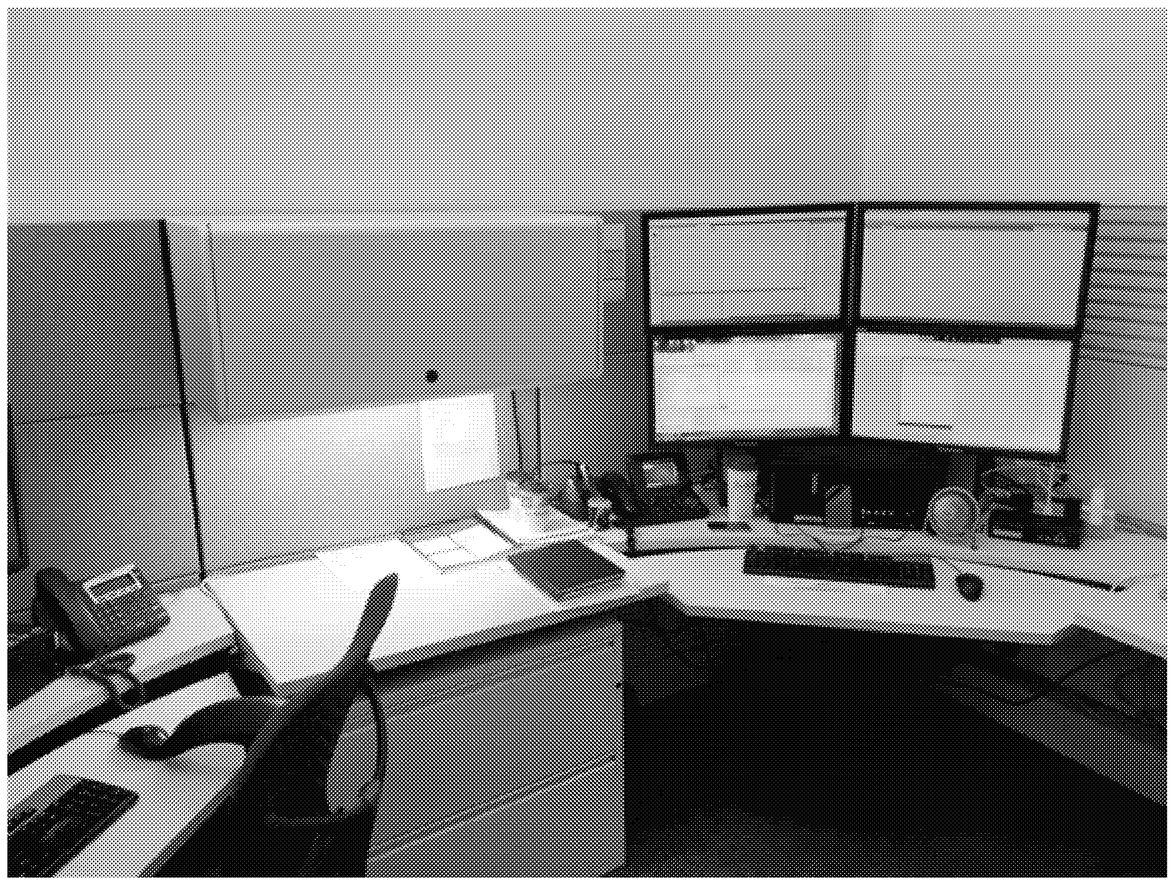

Figure 32. Bruce Powers Computer Security Monitoring Station

The licensee also operates a removable media policy which is underpinned by the enforcement of port blockers and anti-malware scanning kiosks.

During the IPPAS team visit to Bruce Power, the company provided substantial assurances about its computer security awareness program.

Figure 33. Figure 34.

The IPPAS team was assured that the licensee remains committed to deliver assurances which potentially exceed regulatory requirements. For example, during the IPPAS visit the licensee provided details of its approach to mitigating vulnerabilities of IT systems even when they are out of regulatory

scope (such as those which are in the business network and not directly critical to the delivery of operational outputs).

Good Practice: The licensee's commitment to the delivery of a defence-in-depth approach to computer security incorporating constant monitoring and other security processes across both business and operational domains, is worthy of praise.

Bruce Power applies internal requirements for system hardening of its critical digital assets in order to ensure only vital services and network ports are enabled. Where technically feasible, it also mandates that corporate anti-virus solutions must be utilized and all user accounts must be documented with justification in the individual device software maintenance plan.

Finally, the licensee was also able to assure the IPPAS team that, to ensure the integrity of its IT systems, it operates a firm change control process for critical cyber components throughout their life cycle. The change control process involves a collaborative engagement between engineering subject matter experts and their cyber security counterparts, thus delivering substantial assurances across functional specializations.

XVIII.1.5. Computer Access Control

The licensee's assurances relating to access control to IT systems were also highlighted during the IPPAS team's visit. They include restricting access to critical cyber components to those on a 'Security Access List', enforced through technical and management controls. Additionally, the licensee ensures there is no direct access between business and critical operations networks. Rather, access to any critical network is managed and controlled by ensuring connectivity passes through the sanitized Demilitarized Zone (DMZ). The licensee's processes also to contribute to security assurances by ensuring highest classification Critical Cyber Components are inaccessible via network from outside the facilities, including from wireless connectivity.

The licensee was able to assure the IPPAS team that it operates a logical separation of systems, zoned into three areas with layer-3 firewalls, controlled by different departments (thus offering assurances through this segregation of duties). The three zone system operated by the licensee satisfied IAEA minimum recommendations. Notwithstanding these assurances, the IPPAS team gained confidence that the licensee has already identified key areas for improvement of the system.

As far as access to IT systems are concerned, the licensee assured the IPPAS team that access rights are directly linked to clearance levels. Indeed, without an appropriate level of clearance, users are not permitted IT access rights. Conversely, should an active user lose his/her clearance, associated access rights are rapidly deactivated.

Clearances are delivered by the licensee's in-house vetting team. The vetting team accesses vetting databases which are separate to any other system. In addition to the data master clearance record (stored on a separated database), the resultant clearances are maintained in hard copy and archived in locked rooms.

The licensee was also able to confirm that systems administrators who possess privileged access to IT systems - and therefore the potential opportunity to affect the integrity of any such systems - are subject to additional clearance requirements.

Finally, the licensee was able to assure the IPPAS team that it operates a robust education, training and awareness program which includes information and IT security. This includes the use of 'phishing' emails in order to highlight the danger of such messages to the workforce. Should an employee 'click' such an email, they are directed to the licensee's corporate security webpage and encouraged to undertake a security education and awareness program.

XVIII.1.6. Systems Acquisition, Development and Maintenance

With regard to systems acquisition, development and maintenance, the IPPAS team was able to identify the following processes and procedures operated by Bruce Power which contributed to its IT security matrix. For example, Bruce Power assured the team that computer security by design is a concept incorporated into all the licensee's corporate IT development programs. Additionally, Bruce Power aspires to implement full lifecycle management for all its IT systems, including development, design and procurement. However, they suggested that such an approach has not yet been fully introduced across Canada's nuclear industry.

Additionally, at Bruce Power, security architecture and compliance with regulatory requirements are regularly reviewed for new solutions and IT security testing is an essential element of product acceptance. Also, Bruce Power's own guidance mandates that any deployment of new critical cyber components, as well as significant changes, must be executed in a manner which does not adversely affect existing computer security controls, like security patching or software updates.

XVIII.1.7 Incident Management

Robust processes to detect and manage attacks are in operation. The responsibility to manage IT incidents is devolved to the IT security officer who will be supported by an incident response team. The IPPAS team was advised that, in cases where a serious computer incident is identified (e.g. when safety or security objectives may be seriously affected), procedures require an escalation of the responsibility for managing any remediation to their Emergency Preparedness Organization.

Bruce Power employs user reporting in the case of incidents and networked critical components are centrally monitored for security events through the use of intrusion detection systems, network access monitoring, anti-virus software and implementation of system logging. Portable media scans are monitored for evidence of malware.

In accordance with regulatory requirements, reporting of cyber events or IT security issues to CNSC is mandatory. Additionally, licensees may voluntarily report such incidents to the Canadian Cyber Incident Response Centre (CCIRC). Bruce Power advised the IPPAS team that they utilize this opportunity regularly.

XVIII.1.8. Continuity Management

The IPPAS team was advised that, in the event of a loss of availability or integrity, the licensee implements elements of a continuity management process which are part of the specific system design. To complement this response, the licensee has established diversification of systems, where such requirements exist. Additionally, amongst other protection measures, in order to deliver assurances through redundancy, all the licensees' IT systems relevant for the operation of the SMR - including the

access control system - are available in two separate locations (Bruce A and Bruce B). The loss of one of these facilities will be mitigated by the surviving system.

Finally, the licensee assured the IPPAS team that it operates robust recovery plans and procedures for all plant software used for critical computer components. This includes a requirement such plans recovery are tested regularly.

ACKNOWLEDGEMENTS

During the IPPAS mission, the team received outstanding cooperation from personnel at all technical and administrative levels. Indeed, the practical arrangements made by the CNSC 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 team appreciated the openness displayed by those involved in discussing sensitive matters

Throughout the mission, CNSC personnel, the staff of those facilities visited and of all concerned Government organizations, cooperated whole-heartedly with the IPPAS team, generously giving their time, relevant information and kind hospitality. Such untiring assistance - and the timely provision of advance information - helped to make the mission a substantial success. Moreover, the exchange of technical knowledge and experience between the team members, their Canadian counterparts at the CNSC and at the facilities was mutually beneficial.

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

Appendix I: Synopsis of Recommendations, Suggestions and Good Practices

THE RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES ON THE REVIEW OF NATIONAL NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES (MODULE 1):

ON SECTION II (GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION)

II.1.2. Executive Branch

Suggestion: The CNSC should consider Memorandums of Understanding between itself and other Canadian Government departments or agencies, specifically focused on nuclear security responsibilities and functions and (or) consider revising the current MoUs.

II.1.4. Safety, Security and Safeguards in Canada

Suggestion: The CNSC should consider the enhancement of policies and processes which elevate the relative importance of security to ensure it equates with that of safety.

Suggestion: The CNSC should consider reviewing the criteria and performance requirements for an NMAC system for nuclear security purposes to detect an attempt of unauthorized removal (both abrupt and protracted theft) to improve measures against the insider threat.

ON SECTION III (LEGISLATIVE AND REGULATORY FRAMEWORK)

III.2.2. Secondary legislation

Suggestion: From the perspective of an insider adversary, the CNSC should consider amending the Nuclear Security Regulations in order to require at least two nuclear security officers be present in the SMR of High Security facilities at all times; thus minimising the risk of an insider adversary.

Suggestion: On the basis of good international practice, drug and alcohol tests for persons entering the protected area. The CNSC should consider introducing a requirement to perform at least random drug and alcohol tests for persons entering the protected area to ensure they can safely carry out their daily duties.

ON SECTION IV (ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY)

IV.2. Inspection and Enforcement

Recommendation: Taking into account the scale of the Canadian civil nuclear and radiological programme and the wide geographic distribution of regulated entities, the CNSC should review the current security programme to determine the adequacy of resources underpinning its regulatory remit.

ON SECTION V (THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT))

Suggestion: The CNSC should consider introducing a defined timetable for review of the Design Basis Threat, which may deliver a helpful rhythm to the process of updating the document.

Good Practice: The CNSC's maintenance of a dedicated threat intelligence section ensures that the Canadian civil nuclear industry benefits from a mature, well-balanced and comprehensive national intelligence framework, supported by national and international security and intelligence partnerships.

Good Practice: The development, maintenance and utilization of a specific "Adversary force" such as the CATT allows a clear line of understanding amongst licensees of the most likely and most dangerous TTPs of any potential adversary. Such knowledge ensures that training and exercising against Design Basis Threats employ both currency and realism.

Good Practice: The regulatory requirement for a licensee to deliver an annual tactical Threat and Risk Assessment.

Good Practice: The utilization of a classified technology (e.g. secure phone, fax), accessible to suitably cleared licensees complements the rapid and comprehensive dissemination of security updates.

ON SECTION VII (SUSTAINING THE PHYSICAL PROTECTION REGIME)

VII.1. Security Culture

Suggestion: The CNSC should consider using the development of its Management System Safety Culture document as an opportunity to explicitly refer to nuclear security culture and its importance. Useful guidance can be found in IAEA NSS No.7.

Good practice: The CNSC has appointed a dedicated security awareness officer with responsibilities for the security awareness program within the CNSC.

THE SUGGESTIONS AND GOOD PRACTICES ON NUCLEAR FACILITY REVIEW (MODULE 2):

ON SECTION IX (BRUCE POWER NUCLEAR POWER PLANT)

IX.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety

IX.1.3. Interfaces with Nuclear Material Accountancy and Control and Nuclear Safety

Good Practice: Operating a Mobile Operation Centre offers the potential for substantial tactical and operational command and control coherence during any security event or other nuclear emergency.

Suggestion: Joint activities between the safeguards and security personnel should be considered to familiarize both of each other's duties.

IX.1.5. Security Staff Training and Qualification

Good practice: The licensee has a comprehensive training and qualifications program which ensures security staff improve and test their capabilities continuously. It engages the nuclear security officers for continuous development in a motivated way. It also provides motivation for the Nuclear Security Officers in relation to their daily routine.

Good practice: The licensee established and operates a state-of-the-art training facility which focuses on security and emergency personnel operational output.

Good practice: Between the licensee and local police department there is an exceptionally good and close working environment and relationship which ensures a robust mutual understanding of working practices and procedures. This strong relationship extends into the training domain.

IX.1.6. Security Culture

Suggestion:

IX.1.7. Security Procedures

Suggestion: Taking into account federal legislation, the licensee should consider performing random drug and alcohol tests for persons entering the protected area to ensure that they can effectively carry out their daily duties.

IX.1.10. System Evaluation, including Performance Testing

Good Practice: Development and utilisation of a comprehensive 3-D modelling of the facilities allows very substantial opportunities for tactical awareness and understanding on the part of any response force and support the development of tactical deployment plans.

IX.2.3. Access Control

Good practice: The use of systematic explosive checks for all entrants to protected areas is a good practice.

Suggestion:

IX.2.4. Security Monitoring Room (Central Alarm Station)

Suggestion: Bruce Power should consider instituting an exclusion zone for vehicles around the building which houses the SMR. The zone might also benefit from the presence of a functional vehicle barrier.

ON SECTION X (NUCLEAR RESEARCH REACTOR AT McMASTER UNIVERSITY)

X.2.7. Radioactive Source at McMaster – Taylor Source

Suggestion: McMaster should consider applying access control to the reactor airlock doors to provide additional delay.

X.2.4. Security Monitoring Room (Central Alarm Station)

Suggestion: MNR should consider installing a second access control authentication factor, in addition to card access, at some point before access to the SMR.

X.2.6. Response

Good Practice: The McMaster University campus phone application MUSST (McMaster University Safety, Security and Transit) provides important security and emergency response information including for the McMaster Nuclear Reactor.

X.2.7. Radioactive Source at McMaster – Taylor Source

Suggestion: MNR should consider routing the radiation alarm to the SMR to provide additional detection against insider threats.

ON SECTION XI (WESTERN WASTE MANAGEMENT FACILITY OF ONTARIO POWER GENERATION)

XI.1.6. Security Culture

Suggestion: To further promote the importance of Nuclear Security Culture, the licensee should consider formally enshrining its importance by explicitly referring to nuclear security culture, e.g. in values of Code of Business Conduct.

XI.2.3. Access Control

Good practice: The use of systematic explosive checks for all entrants to protected areas is a good practice.

THE SUGGESTIONS ON TRANSPORT REVIEW (MODULE 3):

ON SECTION XII (PHYSICAL PROTECTION MEASURES FOR NUCLEAR MATERIAL DURING TRANSPORT)

XII.2.10. System Evaluation, including Performance Testing

Suggestion: To accord with sound international good practice, CNSC should encourage the development of regular transport security exercises incorporating Design Basis Threat scenarios including on and off-site response forces.

XII.3. Transport Physical Protection System

Good practice: The use of kill switches in vehicles used for the transportation of DSCs is a good practice.

THE RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES ON SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4):

ON SECTION XIII (NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL)

XIII.5. Risk Based Nuclear Security Systems and Measures

Good Practice: The fact that the CNSC registers all five categories of sources in a national database, together with the level of detail of the information that is stored, is a good practice.

XIII.8. Import and Export of Radioactive Material

Good practice: The risk informed and systematic approach, and the level of detail in which the CNSC applies in evaluating requests for export can be considered a good practice. Particular attention is given to the end-use and end-user, safety and security, the importing state, the final and the intermediate consignee, as well as other information from open sources, domestic and foreign watch lists.

ON SECTION XIV.1 (NORDION – KANATA, ONTARIO)

XIV.1.1. Security Management and Security Planning

Good practice: Nordion's strong security management system, which includes an executive security committee and comprehensive security management program, is recognized as a good practice.

XIV.1.4. Intrusion Detection

Suggestion: Nordion should consider the introduction of

XIV.1.5. Alarm Assessment

Suggestion: Nordion should upgrade the window hardness at the SMR as planned.

XIV.1.8. Delay

Suggestion: Nordion should consider

ON SECTION XVI (MITIGATION AND RECOVERY OF NUCLEAR AND OTHER RADIOACTIVE MATERIALS)

XVI.1. Location and Recovery of Missing/Stolen Material

Suggestion: The CNSC should consider making it explicit in the regulations that licensees' contingency plans should include measures to locate and recover any missing and stolen nuclear substances.

THE RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES ON COMPUTER SECURITY REVIEW (MODULE 5):

ON SECTION XVII (COMPUTER SECURITY STATE LEVEL REVIEW)

XVII.1. Legal and Regulatory Framework

Recommendation: CNSC should review the protection afforded to nuclear accountancy and control systems and, if required, enhance regulatory controls to protect them against compromise.

Suggestion: The Regulatory Position Statement from 2008 articulates only that NPPs should satisfy regulatory expectations relating to the implementation of updated and effective computer security management processes. The principles outlined in the 2008 letter should also be extended to cover regulatory expectations for all licensees.

Suggestion: In principle, the coverage and scope of CSA N290.7-14 addresses requirements for robust computer security in nuclear installations. However, the IPPAS team believes it may not necessarily be comprehensive enough to deliver the standards of assurance which accord with evolving regulatory expectations. Accordingly, CNSC should perform a systematic review of the document and decide (potentially on the basis of the 'cyber' DBT and within their own regulatory framework), which modifications or extensions are appropriate.

Suggestion: Based on the defence-in-depth approach, the CNSC should consider codifying minimum standards of IT security practices and processes for non-operational systems and encourage their adoption by all licensees.

Suggestion: CNSC's ongoing activities on risk evaluation and the further development of the DBT should address the relevance of computer related insider threats, due to special attack mechanisms and capabilities.

Suggestion: CNSC should strengthen the protection of sensitive information through certification of a Service Level Agreement with its IT supplier. Additionally, CNSC should require that only GFE be used for CNSC-related work access.

XVII.2. Roles and Responsibilities of Competent Authority

Suggestion: The complexity and scope of the computer security programme requires that CSNC consider reinforcing of relevant human resources.

Good Practice: CNSC regularly undertakes a cross departmental information exchange on the development of computer based threats and vulnerabilities.

Suggestion: CNSC should consider establishing a requirement that licensees must subscribe to the CCIRC threat alert and information capability. Following receipt of an alert, licensees should be required to institute appropriate mitigating actions.

ON SECTION XVIII (COMPUTER SECURITY FACILITY LEVEL REVIEW)

Good practice: The new licensee-initiated formal working group engagements between Canadian civil nuclear licensees for the purposes of ensuring wide understanding of computer based threats, vulnerabilities and associated best practice, is a Good Practice.

XVIII.1.2. Asset Management

Recommendation: The licensee should adapt and extend all relevant documents and procedures to ensure all computer systems used for physical protection are classified as critical digital assets and therefore follow the appropriate computer security processes.

Suggestion: Bruce Power should include auxiliary systems, which might indirectly impact safety or security in their asset management register.

XVIII.1.4. Computer Operations Management

Good Practice: Bruce Power's operation of a comprehensive centralized Computer Security Monitoring Center, which collects relevant information from different networks and domains assists early detection of anomalies or attempts of intrusion.

Good Practice: The licensee's commitment to the delivery of a defence-in-depth approach to computer security incorporating constant monitoring and other security processes across both business and operational domains, is worthy of praise.

Appendix II: IPPAS team Composition

NRC, USA (team leader)
VATESI, Lithuania (legal expert)
ASNO, Australia (research reactor security expert)
ONR, UK (regulatory expert on physical protection of nuclear material & facilities, including security during transport)
STUK, Finland (regulatory expert on physical protection of nuclear material & facilities, including off-site response)
IRSN, France (technical expert on physical protection of nuclear material & facilities)
EnBW Kernkraft GmbH, Germany (computer security expert)
CNCAN, Romania (regulatory expert on physical protection of nuclear material & facilities)
FANC, Belgium (expert on security of radioactive material)
IAEA (mission coordinator)