

**NOTE: This is a sanitized public version of the Mission Report
as edited by ENSI, FOPH and SFOE.**

**Confidential and restricted information have been deleted according to
Swiss legal requirements.**

INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)



INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

IPPAS Follow-up Mission Report: Switzerland

30 October - 10 November 2023

Prepared for the Government of Switzerland

Distribution of this IPPAS follow-up mission report, designated as 'Highly Confidential', is at the discretion of the Government of Switzerland. The IAEA will make the report available to third parties only with the express permission of the Government of Switzerland. 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.

Öffentliche Version vom 21. Mai 2024

ABBREVIATIONS

ADR	European Agreement Concerning the International Carriage of Dangerous Goods by Road
AIP	Advanced Information Package
BNPP	Beznau Nuclear Power Plant
BZL	Federal Interim Storage Facility
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CHUV	University Hospital Lausanne
CPPNM	Convention on the Physical Protection of Nuclear Material
CPPNM/A	Convention on the Physical Protection of Nuclear Material and its 2005 Amendment
CoC	Code of Conduct on the Safety and Security of Radioactive Sources
CSMS	Cyber Security Management System
DBT	Design Basis Threat
DDPS	Federal Department of Defence, Civil Protection and Sport
DRS	Disused Radioactive Sources
DETEC	Federal Department of the Environment, Transport, Energy and Communications
EN	European Standard
ENSI	Swiss Federal Nuclear Safety Inspectorate
ELD	Secure Electronic Platform
FDJP	Federal Department of Justice and Police
Fedpol	Federal Office of Police
FIS	Federal Intelligence Service
FOCBS	Federal Office for Customs and Border Security
FOCP	Federal Office for Civil Protection
FOCS	Federal Office for Cyber Security
FOPH	Federal Office of Public Health
FTE	Full Time Equivalent
GNP	Group of Nuclear Partners
GPS	Global Positioning System
GSKL	Gruppe der Schweizerischen Kernkraftwerksleiter
HASS	High Activity Sealed Sources
HDR	High Dose Rate
HRC	High Radiological Consequences

I&C	Instrumentation & Control
IEC	International Electrotechnical Commission
IAEA	International Atomic Energy Agency
IMS	Integrated Management System
INSServ	International Nuclear Security Advisory Services
INFCIRC	Information Circular
IPO	Information Protection Ordinance
IPPAS	International Physical Protection Advisory Service
IRRS	Integrated Regulatory Review Service
ISO	International Organization for Standardization
IT	Information Technology
ITDB	Incident and Trafficking Database
LNPP	Leibstadt Nuclear Power Plant
MELANI	Reporting and Analysis Center for Information Assurance
MoU	Memorandum of Understanding
MORC	Material out of Regulatory Control
NCSC	National Cyber Security Centre
NDT	Non-Destructive Testing
NEA	Nuclear Energy Act
NEO	Nuclear Energy Ordinance
NEOC	National Emergency Operations Centre
NM	Nuclear Material
NMAC	Nuclear Material Accounting and Control
NPP	Nuclear Power Plant
NSS	IAEA Nuclear Security Series
OAG	Office of the Attorney General
OEF	Operating Experience Feedback
PDCA	Plan, Do, Check, Act
PIN	Personal Identification Number
PPS	Physical Protection System
PSI	Paul Scherrer Institute
PSPV	Ordinance on Personal Security Background Checks
PSPVK	Ordinance on Personal Security Background Checks in the Area of Nuclear Installations
RF	Radio Frequency

RPA	Radiological Protection Act
RPM	Radiation Portal Monitor
RPO	Radiological Protection Ordinance
RPS	Radiation Portal Switzerland
RTS	Representative Threat Statements
SAS	Secondary Alarm Station
SDR	Ordinance on the Transport of Dangerous Good by Road
SFOE	Swiss Federal Office of Energy
SIEM	Security Information and Event Management
SSC	Structures, Systems and Components
SUVA	Swiss National Accident Insurance Fund
SWAT	Special Weapons and Tactics
TA&SM	DETEC Ordinance on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials
TID	Tamper Indicating Device
ToR	Terms of Reference
UAV	Uncrewed Aerial Vehicle
UPS	Uninterruptable Power Supply
UraM	Ordinance of the Federal Department of Home Affairs on the Handling of Radioactive Materials
URC	Unacceptable Radiological Consequences
UUV	Uncrewed Underwater Vehicle
VAPK	Ordinance on the Requirements for the Personnel of Nuclear Installations
VBWK	Ordinance on the Security Guards of Nuclear Installations
VCA	Video Content Analysis
ZWILAG	Central Interim Storage Facility

CONTENTS

ABBREVIATIONS	2
CONTENTS.....	5
SUMMARY.....	11
I. INTRODUCTION.....	13
I.1 Objectives.....	13
I.2 Scope	13
II. RESPONSE TO RECOMMENDATIONS AND SUGGESTIONS PROVIDED DURING THE 2018 IPPAS MISSION	15
II.1 Response to National Level Recommendations and Suggestions.....	15
II.2 Response to Facility Level Recommendations and Suggestions	22
II.2.1 Beznau.....	22
II.2.2 Leibstadt.....	25
II.2.3 Gösgen	26
NATIONAL REVIEW OF NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL (MODULE 1)	27
III. GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION.....	27
III.1 Legislative Branch.....	27
III.2 Executive Branch	28
III.3 Judicial Branch	30
III.4 Safety, Security and Safeguards in Switzerland.....	31
IV. LEGISLATIVE AND REGULATORY FRAMEWORK	33
IV.1 International Instruments.....	33
IV.2 Laws and Secondary Legislation.....	35
IV.2.1 Laws	35
IV.2.2 Secondary legislation – ordinances.....	36
IV.2.3 Regulations and Technical Guidance.....	38
V. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY 40	
V.1 Licensing/Authorization Process.....	42

V.2	Inspection and Enforcement.....	46
V.3	Coordination with Other State Organizations that Contribute to Nuclear Security	47
VI.	THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)	49
VII.	RISK INFORMED APPROACH	51
VII.1	Risk Management.....	51
VII.2	Graded Approach	51
VII.2.1	Definition of Nuclear Material, Nuclear Installation and Radioactive Wastes...	51
VII.2.2	Categorization	52
VII.2.3	Risk of sabotage.....	53
VII.2.4	Interface between the NEA/NEO and the RPA/RPO	54
VII.3	Defence in Depth.....	55
VIII.	SUSTAINING THE PHYSICAL PROTECTION REGIME	56
VIII.1	Security Culture.....	56
VIII.2	Quality Assurance	58
VIII.3	Confidentiality and trustworthiness	59
VIII.3.1	Confidentiality	59
VIII.3.2	Trustworthiness.....	60
VIII.4	Sustainability Programme	60
IX.	PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS	61
IX.1	Contingency Planning at the National Level.....	61
IX.2	Emergency and Contingency Planning Interface	62
	NUCLEAR FACILITY REVIEW (MODULE 2)	64
X.	NPP Leibstadt.....	64
X.1	Security Management Programme	64
X.1.1	Threat and Target Identification	64
X.1.2	Security Plan, including Contingency Plan	64
X.1.3	Security Organization	65
X.1.4	Security Staff Training and Qualification.....	65
X.1.5	Security Culture	65
X.1.6	Interfaces with Nuclear Safety and Nuclear Material Accounting and Control .	65
X.1.7	Security Procedures	65
X.1.8	Confidentiality and Trustworthiness.....	65

X.1.9	Reporting of Nuclear Security Events	66
X.1.10	System Evaluation, including Performance Testing	66
X.1.11	Quality Assurance	67
X.1.12	Sustainability Programme	67
X.2	Physical Protection System	68
X.2.1	Graded Protection and Defence in Depth	68
X.2.2	Detection	68
X.2.3	Access Control	69
X.2.4	Central Alarm Station	69
X.2.5	Delay	70
X.2.6	Response	70
XI.	ZWILAG	71
XI.1	Security Management Programme	71
XI.1.1	Threat and Target Identification	71
XI.1.2	Security Plan, including Contingency Plan	72
XI.1.3	Security Organization	72
XI.1.4	Security Staff Training and Qualification	73
XI.1.5	Security Culture	73
XI.1.6	Interfaces with Nuclear Safety and Nuclear Material Accounting and Control .	73
XI.1.7	Security Procedures	73
XI.1.8	Confidentiality and Trustworthiness	73
XI.1.9	Reporting of Nuclear Security Events	74
XI.1.10	System Evaluation, including Performance Testing	74
XI.1.11	Quality Assurance	74
XI.1.12	Sustainability Programme	74
XI.2	Physical Protection System	74
XI.2.1	Graded Protection and Defence in Depth	74
XI.2.2	Detection	75
XI.2.3	Access Control	76
XI.2.4	Central Alarm Station	77
XI.2.5	Delay	77
XI.2.6	Response	77
	TRANSPORT REVIEW (MODULE 3)	78
XII.	TRANSPORT SECURITY LEGISLATION AND REGULATIONS	78
XIII.	TRANSPORT SECURITY MANAGEMENT	78

XIII.1	Threat and Target Identification.....	79
XIII.1.1	Allocation of Responsibilities.....	79
XIII.1.2	Transport Security Plan, including Contingency Plan.....	80
XIII.1.3	Interfaces with Nuclear Material Accounting and Control and Nuclear Safety .	80
XIII.1.4	Security Staff Training and Qualification.....	80
XIII.1.5	Security Culture.....	80
XIII.1.6	Trustworthiness.....	80
XIII.1.7	Reporting of Nuclear Security Events.....	80
XIII.1.8	System Evaluation, including Performance Testing.....	80
XIII.1.9	Quality Assurance.....	80
XIII.1.10	Sustainability Programme.....	80
XIII.1.11	Confidentiality.....	80
XIII.2	Transport Physical Protection System.....	81
XIII.2.1	Graded Protection and Defence in Depth.....	81
XIII.2.2	Detection.....	81
XIII.2.3	Transport Control Centre.....	81
XIII.2.4	Delay.....	81
XIII.2.5	Response.....	81
SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4).....		82
XIV.	NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL.....	82
XIV.1	Assignment of Nuclear Security Responsibilities.....	82
XIV.1.1	State.....	82
XIV.1.2	Regulatory body.....	82
XIV.1.3	Other Competent Authorities.....	85
XIV.1.4	Operator, Shipper and/or Carrier.....	88
XIV.2	Legislative and Regulatory Framework.....	88
XIV.2.1	Laws.....	89
XIV.2.2	Ordinance.....	90
XIV.2.3	FOPH Guideline.....	91
XIV.2.4	Trustworthiness verification.....	93
XIV.2.5	National Registry and Inventory of Radioactive Sources.....	94
XIV.3	International Cooperation and Assistance.....	95
XIV.4	Identification and Assessment of Threats.....	96
XIV.5	Risk Based Nuclear Security System and Measures.....	96

XIV.5.1	Risk Management	96
XIV.5.2	Interface with the Safety System	97
XIV.6	Sustaining the Nuclear Security Regime.....	97
XIV.7	Planning and Preparedness for and Response to Nuclear Security Events	98
XIV.8	Detection and Reporting Nuclear Security Events.....	100
XIV.9	Import and Export of Radioactive Sources	102
XIV.10	Management of Disused Radioactive Sources	102
XIV.11	Security of Radioactive Material in Transport.....	103
XIV.11.1	Transport security requirements and regulations	103
XIV.11.2	Security Management and Transport Security Plan.....	103
XIV.11.3	Implemented Detection, Delay and Response Measures	105
XIV.11.4	International Transport.....	105
XV.	FACILITY LEVEL REVIEW	106
XV.1	LorNDT	106
XV.2	Security Management.....	106
XV.2.1	Graded Protection and Defence in Depth	107
XV.2.2	Trustworthiness Verification	107
XV.2.3	Protection of Sensitive Information	107
XV.2.4	Security Plan	107
XV.2.5	Contingency Plan	108
XV.2.6	Reporting Security Events	108
XV.2.7	Location and Recovery of Missing/Stolen Material	108
XV.2.8	Measures to Mitigate/Minimize Radiological Consequences of Sabotage.....	108
XV.3	Security System.....	109
XV.3.1	Detection and Alarm Assessment	109
XV.3.2	Delay	111
XV.3.3	Response	112
XV.3.4	Emergency Power Supply	113
XV.3.5	Locks and Keys	113
XVI.	University Hospital Lausanne (CHUV).....	114
XVI.1	Security Management.....	115
XVI.1.1	Graded Protection and Defence in Depth	115
XVI.1.2	Trustworthiness Verification	115
XVI.1.3	Protection of Sensitive Information	116
XVI.1.4	Security Plan	116

XVI.1.5	Contingency Plan	116
XVI.1.6	Reporting Security Events	117
XVI.1.7	Location and Recovery of Missing/Stolen Material	117
XVI.1.8	Measures to Mitigate/Minimize Radiological Consequences of Sabotage.....	117
XVI.2	Security System.....	117
XVI.2.1	Detection and Alarm Assessment	117
XVI.2.2	Access Control	121
XVI.2.3	Delay	122
XVI.2.4	Response	123
XVI.2.5	Emergency Power Supply	124
XVI.2.6	Locks and Keys	124
COMPUTER SECURITY REVIEW (MODULE 5).....		125
XVII.	COMPUTER SECURITY STATE LEVEL REVIEW.....	125
XVII.1	Legal and Regulatory Framework.....	125
XVII.2	Roles and Responsibilities of the Competent Authority	126
XVIII.	COMPUTER SECURITY FACILITY LEVEL REVIEW	129
XVIII.1	Computer Security at NPP Gösgen	129
XVIII.2	Computer Security at NPP Leibstadt	129
ACKNOWLEDGEMENTS.....		130
APPENDIX I: SYNOPSIS OF RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES.....		131
APPENDIX II: IPPAS TEAM COMPOSITION.....		137
APPENDIX III: HOST COUNTRY COUNTERPARTS.....		138

SUMMARY

For this IPPAS mission the IAEA assembled a nine-person team comprised of experts from eight nations and the IAEA. The experts have broad expertise and experience in nuclear legislation, regulatory oversight, physical protection system design, implementation and assessment, including security during transport of nuclear material, security of radioactive material, associated facilities and activities, and computer security.

During the mission, the IPPAS team interacted and discussed with key representatives from the Federal Department of Environment, Transport, Energy and Communications, the Swiss Federal Nuclear Safety Inspectorate, the Swiss Federal Office of Energy, the Swiss Federal Office of Public Health, the Federal Intelligence Service, the National Cyber Security Center, the Federal Police, the Police from Canton Aargau, as well as the management and staff of the visited nuclear power plants of Leibstadt and Beznau, the Central Interim Storage Facility ZWILAG, and facilities associated with radioactive materials: University Hospital of Lausanne (CHUV) and LorNDT, in Sâles.

It was apparent to the IPPAS team that a significant amount of time and effort was invested by the Swiss representatives in the preparation and conduct of the mission. The host country provided the IAEA and the IPPAS team members with an Advanced Information Package consisting of relevant information related to the legislative and regulatory framework, roles and responsibilities of the competent authorities, as well as information on the technical characteristics of the nuclear power plants.

As a result of the 2018 IPPAS Mission, a total of 13 good practices, 9 recommendations and 37 suggestions were identified. Progress against the recommendations and suggestions was assessed by the 2023 follow-up mission and it is concluded that five of the recommendations are fully implemented and closed and four are addressed but will remain open until actions are fully implemented. Of the suggestions from the 2018 mission 31 are considered implemented and are closed and six remain open until the planned actions are fully implemented. As a result of the review of the status of recommendations and suggestions from the 2018 IPPAS mission, one new recommendation (R1) and three new suggestions (S7, S11 and S36) were identified by the IPPAS team.

The scope of the 2023 IPPAS follow-up mission included Modules 1 to 5 as described in the IAEA Service Series 29 (IPPAS Guidelines). Module 4 on the Security of radioactive material, associated facilities and associated activities was not included in the scope of the 2018 IPPAS mission to Switzerland and was reviewed by the IPPAS team for the first time during the 2023 follow-up mission.

As a result of the IPPAS follow-up mission in 2023, the IPPAS team has identified a total of 17 good practices, 18 recommendations and 39 suggestions. Most of these relate to Module 4 with a total of 14 good practices, 13 recommendations and 16 suggestions.

Some examples of good practices are: Competent Authorities' frequent and active participation in international forums and peer reviews teams; The success and accomplishment of the RADISS Action Plan; High level of technical competency of ENSI nuclear cyber security team; the implementation of several nuclear security measures beyond the requirements in facilities associated with other radioactive material as well as in some nuclear facilities, etc.

The recommendations in Module 1 refer inter alia to:

- the establishment of NMAC requirements for nuclear security purposes,
- improvement in the interchange of information between competent authorities,
- clarification of the conditions to distinguish the need of a permit or a licence amendment for a modification affecting nuclear security,
- Assessment of categorization process for protection of any quantity of nuclear material against unauthorized removal, and
- Graded approach for protection of nuclear material and SSC against sabotage.

The recommendations in Module 4 refer to different issues, such as:

- Training program for inspectors from FOPH and SUVA,
- continuation of promotion of nuclear security culture for other radioactive material
- sustainability of the achievements of the RADISS plan through the allocation of sufficient human and financial resources,
- Establishment of national contingency plan to response to malicious acts,
- National strategy for the management of disused HASS, and
- National strategy for detection of MORC.

The suggestions provided by the IPPAS team are based on international good practices and IAEA Nuclear Security Series implementing guides and technical guides, in order to support Switzerland enhancing and sustaining nuclear security of nuclear material and other radioactive material.

The IPPAS team commends the extraordinary work that has have been undertaken by the small team of FOPH and SUVA experts and congratulates them on their achievements in the enhancement of the security of HASS.

The IPPAS team also observed that the nuclear security regime in Switzerland is robust and well-established and incorporates the fundamental principles of the CPPNM and its 2005 Amendment, as well as CoC and that the nuclear security regime has been substantially enhanced since the last IPPAS mission in 2018 based on the continuous improvement principle applied by the Swiss authorities.

In conclusion, the IPPAS team assessed that Switzerland is making further significant efforts towards the enhancement of its national nuclear security regime and that the IPPAS follow-up mission was an additional step in that direction.

I. INTRODUCTION

This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) follow-up mission conducted from 30 October to 10 November 2023 at the request of the Government of Switzerland.

I.1 Objectives

The first objective of the IPPAS follow-up mission was to review the status of the findings from the 2018 mission, and to provide the IPPAS team's response to those. Conclusions are included in this report. The second objective was to review the current status of Swiss national nuclear security through a comparison with the obligations specified under the CPPNM and its 2005 Amendment, the Nuclear Security Fundamentals (NSS No. 20) and the consensus recommendations defined in NSS No. 13 (also known as INFCIRC/225/Rev.5). The third objective was to review the current status of the Swiss national nuclear security through a comparison with the obligations specified under the Code of Conduct on Safety and Security of Radioactive Material, NSS No. 14 (Security of Radioactive material, associated facilities and associated activities) and other relevant IAEA Nuclear Security Series guidance in relation to Module 4, which was not covered during the mission in 2018. Respectively, the findings for this module are presented in this report. New findings for other modules are introduced under each respective module in this follow-up mission report.

I.2 Scope

The scope of the IPPAS follow-up mission included the following modules of the IPPAS Guidelines (IAEA Services Series 29):

- Module 1 (National Review of Nuclear Security Regime for Nuclear Material and Nuclear Facilities);
- Module 2 (Nuclear Facility Review);
- Module 3 (Transport Review);
- Module 4 (Security of Radioactive Material, Associated Facilities and Associated Activities);
- Module 5 (Computer Security Review).

The following competent authorities were interviewed during the IPPAS follow-up mission:

- Swiss Federal Nuclear Safety Inspectorate (ENSI);
- Federal Office of Public Health (FOPH);
- Swiss Federal Office of Energy (SFOE);
- Federal Department of the Environment, Transport, Energy and Communications (DETEC)
- Swiss National Accident Insurance Fund (SUVA);
- National Cyber Security Centre (NCSC);
- Federal Intelligence Service (FIS);
- Federal Police;

- Cantonal Police Aargau, and
- Cantonal Command Staff

The following nuclear facilities were visited during the IPPAS follow-up mission:

- Nuclear Power Plant Beznau;
- Nuclear Power Plant Leibstadt, and
- Central Interim Storage Facility (ZWILAG)

The following associated facilities for radioactive material were visited during the IPPAS follow-up mission:

- University Hospital of Lausanne (CHUV), and
- LorNDT, Sâles

II. RESPONSE TO RECOMMENDATIONS AND SUGGESTIONS PROVIDED DURING THE 2018 IPPAS MISSION

This chapter aims to summarize the recommendations and suggestions provided during the IPPAS Mission conducted in 2018, the responses provided in the presentations delivered by experts and their updates provided during and after the discussion with the IPPAS team, as well as the evaluation of the progress made by the IPPAS team.

II.1 Response to National Level Recommendations and Suggestions

Recommendation 1 (2018): The State should establish thresholds of unacceptable radiological consequences (URC) in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection.

The IPPAS team was informed that ENSI has considered several approaches to address Recommendation 1 and considers revision of the design basis threat (DBT) as a possible solution to introduce URC thresholds. In addition to the above, ENSI also mentioned that the revised DBT could include the possibility to address different classes of nuclear facilities at different stages of life cycle following a graded approach.

The IPPAS team concludes that Recommendation 1 is still being considered and will be addressed after implementation of the abovementioned strategy. This recommendation remains OPEN.

Recommendation 2 (2018): The ENSI and the SFOE should identify and agree the interfaces between nuclear security and safeguards. Once agreed, the ENSI and the SFOE should work together to develop requirements, procedures and processes to facilitate mutually supportive measures for both safeguards and security purposes.

The IPPAS team was informed that ENSI and SFOE have been discussing the interfaces between security and safeguards and that there is a working group on “3S” (safety, security and safeguards) that meets regularly and in which FOPH is also present. The cooperation between these three entities has not been formalized through Memorandum of Understanding (MoU) or Terms of Reference (ToR). Cooperation between the different stakeholders having responsibilities for nuclear security and safeguards in Switzerland is based on discussions and the IPPAS team recognised the fact that the responsible persons know each other, which allows good cooperation. The challenge in this approach is that if the responsible persons change for any reason, present cooperation might be endangered. Even if, the IPPAS team did not find any evidence that cooperation is currently not working, the team considers that for continuity and sustainability, it would be worth considering formalising such cooperation e.g., in the form of MoU or ToR. This topic is discussed more under Chapter III.4 below.

The IPPAS team concludes that the first part of this recommendation 2 has been considered and remains OPEN until the implementation of the proposed new Suggestion 2 under Chapter III.4 below.

The second part of Recommendation 2 discusses Nuclear Material Accounting and Control (NMAC) for nuclear security purposes. During the follow-up mission, the IPPAS team recognised that assessment of NMAC related measures for nuclear security purposes and possible need of requirements for operators have not been conducted by ENSI. To address the insider threat in particular in certain type of nuclear facilities (such as Paul Scherrer Institute, PSI), an assessment of NMAC measures, insider threat

risks and possible requirements in this area for the timely detection of insider threat should be undertaken.

The IPPAS team concludes that the second part of this recommendation 2 has been considered and is CLOSED. The new Recommendation 1 regarding NMAC for nuclear security purposes is under Chapter III.4 below.

Recommendation 5 (2018): The ENSI should evaluate and review the radiological consequences of possible sabotage scenarios, including insider and external adversary threats against the transport of nuclear materials, should compare the result to the established URC and should decide on the necessity of physical protection measures additional to that provided by the safety features of the design of the transport package, container and conveyance.

The IPPAS team was informed that since the last mission in 2018 a DBT for transport has been developed and is described in the recently introduced guideline ENSI-B15 – ‘Security Measures for Nuclear Material and Radioactive Waste in Transport’. In addition, in order to understand the consequences of a ballistic attack, ENSI has undertaken studies with the FIS and defence companies and has also reviewed and updated an existing study of the effects of a kinetic attack on a transport cask.

It still remains open, however, as since the State has not defined the level of URC, no analysis can be performed to assess if additional nuclear security requirements would be needed for protection against possible sabotage scenarios against nuclear material during transport. It remains the case that the cantonal police decide upon the necessary security measures needed during the transport based on their threat assessment and the category of the nuclear material and although there is no legal requirement for the police to escort a transport, the IPPAS team was informed that in practice the transports of Category I and II nuclear materials are always escorted by the police.

The IPPAS team concludes that this Recommendation 5 is being considered in relation to Recommendation 1 (2018). This recommendation remains OPEN.

Recommendation 6 (2018): The State should unambiguously assign the prime responsibility of holding a license for the transport of nuclear material to a single legal entity, not to all stakeholders involved in a particular transport activity. The responsibility of the shipper, the carrier, the receiver and the transport organization should also be explicitly stipulated in the regulation.

It was explained to the IPPAS team that ‘joint responsibility’ is a Swiss principle and therefore the relevant legislation will not be amended, however, there is now a requirement in guideline ENSI-B15 that stipulates that a single entity for the transport security plan should be designated.

The IPPAS team concludes that the objective of Recommendation 6 has been considered and is CLOSED.

Recommendation 7 (2018): The State should require the shipper and/or carrier, as appropriate, to submit a transport security plan for approval by the ENSI prior to the transport of Category I and II nuclear material.

The IPPAS team was informed that there is now a requirement in guideline ENSI-B15 for the submission of a transport security plan for approval by ENSI for moves of Category I and II nuclear material.

The IPPAS team concludes that Recommendation 7 has been implemented and is CLOSED.

Recommendation 8 (2018): The ENSI should establish nuclear computer security regulatory requirements at a high level to ensure effective and measurable provisions consistent with the threat assessment and design basis threat.

The IPPAS team has reviewed the contents of the ENSI-G22/e Cyber Security in Nuclear Installations, Guideline for Swiss Nuclear Installations, and concludes that it successfully addresses the intent as stated above.

The IPPAS team concludes that Recommendation 8 has been implemented and is CLOSED.

Recommendation 9 (2018): The ENSI should consider extending its regulatory oversight in the area of NMAC in order to ensure that NMAC systems are effectively protected against computer security related threats.

The IPPAS team was informed that the operators of the Nuclear Power Plants (NPP) have discussed the interface between nuclear security and NMAC. In addition, ENSI has conducted computer security inspections on NMAC systems at two NPPs.

The IPPAS team concludes that Recommendation 9 has been implemented and is CLOSED.

Suggestion 1 (2018): The ENSI should consider establishing an advisory committee in the field of nuclear security.

The IPPAS team was informed that different competent authorities (Group of Nuclear Partners, GNP) meet regularly. GNP makes no decisions, nor official statements. Formalising cooperation in the nuclear security sector is discussed more under Chapter III.4 below. The IPPAS team concludes that Suggestion 1 has been considered and is CLOSED.

Suggestion 2 (2018): The State should consider accelerating the finalisation of the review of its implementation of the CPPNM/A and, in accordance with Article 14 of the CPPNM/A, informing the CPPNM/A's depository of its laws and regulations which give effect to the CPPNM/A.

The IPPAS team was informed that the review has been done and the IPPAS team observed that in 2021 Switzerland officially informed the CPPNM/A's depository of its laws and regulations which give effect to the CPPNM/A. The IPPAS team concludes that Suggestion 2 has been implemented and is CLOSED.

Suggestion 3 (2018): The State should consider the consistent use of the terms nuclear security and nuclear safety when defining legal requirements in areas where a distinction is made in the level of implementation by the competent authorities and the operators.

The IPPAS team was informed that whenever the legislation is revised or amended, this suggestion is taken into account by ENSI.

It was observed by the IPPAS team that in Swiss laws, ordinances and various guidelines and other documentation the use of the terms 'nuclear safety' and 'nuclear security' is inconsistent. In some areas it is specified that nuclear safety incorporates nuclear security but in other areas this is not the case. This has the potential for confusion both at the national and international level and could challenge effective management when planning and implementing different programmes and activities. There is, therefore, the need for a common understanding and common terminology for these concepts.

The IPPAS team concludes that Suggestion 3 has been considered and is CLOSED regarding ENSI, as ENSI systematically implements it.

Suggestion 4 (2018): In line with the relevant recommendation provided by the IRRS mission in 2015, the State should consider modifying the legal status of nuclear security requirements to ensure that they are legally binding per se in order to avoid the need to base their binding character on other circumstances.

The IPPAS team was informed that the IRRS follow-up mission to Switzerland in 2015 covered this topic. Under Recommendation 6 of that mission report it is concluded that the recommendation has not been fully addressed and is superseded by recommendation RF1 which recommends that *ENSI's independency should be strengthened by giving ENSI the ability to issue binding [...]*.

The IRRS mission report 2021 does not discuss Recommendation RF1 further. Therefore, the IPPAS team considers that Suggestion 4 is CLOSED.

Suggestion 5 (2018): The State should consider allowing prosecution of a licensee that could result in pertinent sanctions (e.g., fines) in order to fully reflect the prime responsibility of licensees for nuclear security and to balance the enforcement measures (sanctions) between licensees and individual natural persons.

The IPPAS team was informed that the IRRS follow-up mission to Switzerland in 2015 covered this topic. Under Recommendation 9 of that mission report it is concluded that the recommendation is open: *ENSI has taken a number of initiatives for dialogue with the ministries, and discussions are still ongoing. The ultimate responsibilities for resolving the issues with the legal framework is with the Government to revise the law to be consistent with IAEA Safety Standards.*

The IPPAS team concludes that the Suggestion 5 has been considered and is covered in the IRRS mission report 2015 at a higher level (recommendation). The topic is also covered by Recommendation 4 of the 2021 IRRS mission report. Therefore, there is no need for a suggestion and the team considers that Suggestion 5 is CLOSED.

Suggestion 6 (2018): The FIS should consider performing a specific nuclear security threat assessment, and preparing and maintaining a nuclear security threat assessment document, including cyber threats, which can provide input for the development of the facility specific design basis threat.

The IPPAS team was informed that FIS does not develop and maintain domain specific threat assessments and does not consider it would be needed. In addition, the IPPAS team was informed that threat assessment information from FIS is delivered through discussions between FIS and ENSI.

The IPPAS team observed that FIS is responsible for the national threat assessment according to Art. 6 of the Intelligence Service Act of 2015. According to Art. 7 of the DETEC Ordinance on Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials of 2008, FIS keeps ENSI informed of any changes to the national threat assessment.

According to Art. 3 of the DETEC Ordinance on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials, the national threat assessment could be used by ENSI to develop the Design Basis Threat, however, FIS does not produce a specific nuclear sector threat assessment. ENSI has defined the DBT in its guideline ENSI-A09 DBT for nuclear facilities. With respect to cyber security (computer security according to IAEA terminology) the DBT also includes aspects related to IT systems as targets or attack paths. Further details of the cyber DBT may be found in guideline ENSI-G22 'Cyber Security'.

It has been found that there is no documented national threat assessment, as recommended in IAEA NSS No. 10-G. The national threat assessment should be used to inform the implementation of the state's nuclear security regime, in particular, there should be an evaluation by the state of the threat of unauthorized removal and of sabotage. This is fundamental when developing the DBT, the purpose of which is to articulate a common basis for the design and implementation of the physical security system. A documented threat assessment provides a historical foundation for the DBT and the underpinning rationale should there be a requirement to make changes.

The IPPAS team concludes that the Suggestion 6 has been considered and is CLOSED. However, taking into account the importance of threat assessment for developing a DBT, the IPPAS team considers documented threat assessment is relevant for DBT. This topic is discussed more under new Suggestion 7 in Chapter VI below.

Suggestion 7 (2018): The ENSI should consider requiring the operators to develop a generic series of pre-determined nuclear security measures for each response level, which should be implemented by the license holder in the event that there is a sudden increase in the threat level.

The IPPAS team was informed that this matter has been addressed in ENSI-G09, chapter 5.6. In addition, the operators already have pre-determined nuclear security measures for each response level in place.

The IPPAS team concludes that Suggestion 7 has been implemented and is CLOSED.

Suggestion 8 (2018): The State should consider developing requirements for a more extensive range of preventive and protective measures to mitigate the insider threat at nuclear facilities.

The IPPAS team was informed that there are no specific legal provision addressing explicitly insider threat, but that ENSI is aware of this topic. In addition, it was explained to the team that typical preventive and protective measures, such as a two-person rule are implemented by facility operators through procedures. It is also covered in the DBT. In addition, ENSI-G22 includes e.g., a requirement for the two-person rule in certain applications of security measures.

The IPPAS team concludes that Suggestion 8 has been considered and certain actions have been implemented and it is CLOSED.

However, taking into account the importance of measures against the insider threat in particular in relation to NMAC, this topic is discussed more below under Chapter III.4 (new Recommendation 1).

Suggestion 9 (2018): The State should consider increasing the regularity of the review process of the DBTs.

The IPPAS team was informed that there is a requirement for guidelines to be assessed annually to identify the possible need for a review. This is documented through the management system of ENSI.

The IPPAS team concludes that Suggestion 9 has been implemented and is CLOSED.

Suggestion 10 (2018): The ENSI should consider facilitating the sharing of relevant parts of the facility specific DBTs with the cantonal police forces in order to inform their response.

The IPPAS team was informed that ENSI provides the cantonal police forces with the DBT. The facility specific DBTs are not significantly different from this DBT and there is no recognised reason for the facility specific DBTs to be held by the cantonal police. The facility specific DBT is a sub-set of the State DBT.

The IPPAS team concludes that Suggestion 10 has been addressed and is CLOSED.

Suggestion 11 (2018): The ENSI should consider completing the relevant guideline and issuing it as soon as possible in order that clearly defined performance testing is included in the evaluation of the physical protection system.

The IPPAS team was informed that guideline ENSI-A12 is still in the drafting process and upon publication of the guideline, this suggestion will be addressed.

The IPPAS team concludes that Suggestion 11 has been considered and remains OPEN until the publication of ENSI-A12 and its implementation at the facility level.

Suggestion 12 (2018): The ENSI should consider requiring all license holders to perform nuclear security culture self-assessments and to address the areas of improvement in a structured enhancement programme.

The IPPAS team was informed that guideline ENSI-G07 includes requirements for safety culture and the explanatory memorandum explains self-assessment of safety culture is one provision to enhance safety culture. However, there is no specific requirement to conduct self-assessment. In addition, it was explained to the IPPAS team that safety culture includes security culture. ENSI's activities in the oversight of culture for safety includes security culture and the implementation in the nuclear facilities is subject to follow-up by ENSI's experts in the field.

The IPPAS team concludes that this Suggestion 12 has been addressed by implementing activities by the facility operators and new revision of ENSI-G07 further emphasizes the topic. Based on the information above, the IPPAS team concludes Suggestion 12 is CLOSED.

Taking into account that the basis for security culture is the recognition that a credible threat exists, nuclear security is important and everybody working in this sector has a role in nuclear security, it should be further promoted. That can be demonstrated, for example, in a Nuclear Security Policy. The topic is discussed more in new Suggestion 12 under Chapter VIII.1.

Suggestion 13 (2018): The State should consider broadening the objectives within the relevant ordinance to cover the protection of security relevant information.

The IPPAS team was informed that the State has revised major parts of its security framework and has introduced new legislation for the protection of information. Several subordinated ordinances were adjusted accordingly. Within guideline ENSI-G09, the information protection requirements were adjusted to be in line with the new legal requirements which shall come into force in 2024.

The IPPAS team concludes that Suggestion 13 has been addressed (at the State level) and that ENSI has revised its guideline ENSI-G09 to reflect the new legislation. Suggestion 13 will remain OPEN until the new legislation comes into force.

Suggestion 14 (2018): The ENSI should consider performing an adequate number of unannounced security inspections in their regulatory inspection programme.

The IPPAS team was informed that unannounced inspections have been carried out and they are part of the annual inspection planning.

The IPPAS team concludes that Suggestion 14 has been implemented and is CLOSED.

Suggestion 15 (2018): The ENSI should consider formalising the use of ‘force-on-force’ exercises in order that the response forces train against a realistic, dynamic adversary.

The IPPAS team was informed that ENSI has recognised there is a missing link between the DBT and physical protection implementation regarding scenarios. Therefore, ENSI has drafted a sabotage scenario development procedure and presented a “model scenario” for the operators during a workshop. ENSI is in a process to formalize a sabotage scenario development procedure. The topic is discussed more under Recommendation 3 (2018) below.

The IPPAS team concludes that this Suggestion 15 in relation to Recommendation 3 (2018) is being considered and remains OPEN until publication and implementation of the scenario development procedure by the facility operators.

Suggestion 23 (2018): The ENSI should consider communicating the potential radiological consequences of transport sabotage targets to the response forces, who should consider implementing the appropriate measures.

The IPPAS team was informed that since this suggestion ENSI have held a workshop with the cantonal police to discuss the potential radiological consequences of an attack on a transport cask. The cantonal police have now developed training for those officers involved in escorting transport moves to cover this area and the immediate actions to take in such an event to maintain public safety.

The IPPAS team concludes that Suggestion 23 has been implemented and is CLOSED.

Suggestion 24 (2018): The State should consider requiring trustworthiness verification for all personnel involved in the transportation of Category I and II nuclear material, including personnel of non-state organizations, as a preventive measure against insider threats.

The IPPAS team was informed that the PSPVK requires background checks only on persons with security functions within nuclear facilities. However, ENSI-B15 now specifies that persons involved in the transportation of nuclear material with access to information classified as CONFIDENTIAL or SECRET must have a trustworthiness declaration based on personnel security vetting. The trustworthiness of the other participants is ensured by appropriate checks; however, these are not specified and it is, therefore, unclear if the background of the drivers, who may pose relevant security risks as insiders, is effectively assessed.

The IPPAS team was informed by ENSI that there is no legal basis or appetite from the federal authorities to require the personnel security vetting of persons involved in the transportation of nuclear material other than for those with a security function. However, ENSI-B15 directs that the consignor is responsible for ensuring that other persons involved in a transport move, such as the driver, have a background check.

The IPPAS team concludes that Suggestion 24 has been considered as far as possible and is CLOSED.

Suggestion 25 (2018): In addition to table top transport exercises, the relevant competent authorities, including the off-site response force, together with the operators, shippers and carriers should consider organising regular transport security field exercises.

The IPPAS team was informed that transport exercises have been planned, but not conducted yet. Suggestion 25 remains OPEN.

Suggestion 26 (2018): The ENSI should consider issuing a guideline on transport security requirements that is in compliance with NSS 13, taking into account NSS 26-G.

The IPPAS team was presented information showing that a new guideline has been developed to cover transport security requirements (Guideline ENSI-B15 - Security Measures in The Transport of Nuclear Material and Radioactive Waste). The guidelines apply to the transportation of Category I, II and III nuclear material and radioactive waste and clearly set out the security requirements for all relevant stakeholders and cover responsible persons, escorting, application of the DBT and exercising.

The IPPAS team concludes that Suggestion 26 has been implemented and are CLOSED.

Suggestion 27 (2018): The ENSI should consider establishing criteria for classification of security or security related digital systems in line with NSS 17 Para 5.4.2.

The IPPAS team concludes that Suggestion 27 has been implemented within ENSI-G22 and is CLOSED.

Suggestion 28 (2018): The ENSI should consider creating a security capability within its staff, to understand vehicle vulnerabilities and to ensure technical understanding of the threat to future transport shipments and fleet vehicles from cyber based attack, and then proactively adjust guidance to effectively address the threat.

The team acknowledges that ENSI is aware of this topic and has evaluated it in the development of the transport security guideline. Based on the information above, the IPPAS team considers that Suggestion 28 is CLOSED. However, given the complex assignment of regulatory and oversight security responsibilities around the transport function, this topic is discussed more under Chapter XIII.2 below.

Suggestion 29 (2018): The ENSI should consider establishing content within the pending Guideline ENSI-G22 that takes into account the identification of both risk-based security levels and their affiliated requirements as well as a separate designation for administrative groupings of computers that operate within a similar security level or what is commonly referred to as a “zone

The IPPAS team has reviewed and acknowledges the incorporation of “zones” as a security management component of risk base defined “levels” within ENSI-G22 and considers this Suggestion 29 is CLOSED.

II.2 Response to Facility Level Recommendations and Suggestions

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

III. GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION

Switzerland is a well-developed federal state which operates under a unique and decentralized federal system with a strong emphasis on direct democracy. The political system of Switzerland is based on the broad cooperation of public entities and long tradition of direct democracy on federal, cantonal and also local level. Its constitutional framework is outlined in the Federal Constitution of the Swiss Confederation, which was adopted in 1848 and subsequently revised several times. The Federal structure comprises 26 cantons, each with a significant degree of autonomy in matters not explicitly assigned to the federal government (subsidiary principle).

In the event of conflict, federal law takes precedence over any conflicting provision of cantonal law and the Federation must also ensure that the cantons comply with federal law (Article 49 of the Federal Constitution).

III.1 Legislative Branch

The legislative branch in Switzerland is bicameral in order to balance the interests of the individual cantons and the Swiss population and is vested in the Federal Assembly. The Federal Assembly consists of The National Council and The Council of States. The National Council is composed of 200 members on a system of proportional representation. The Council of States is the upper house of the Federal Assembly and is composed of 46 members, with each canton being represented by two members and six half-cantons by one member.

The direct democracy system enables Swiss citizens to put laws that have already been passed by parliament to a popular vote and to put a constitutional amendment to a popular vote by means of a popular initiative. Constitutional amendments proposed by parliament must also be approved by a popular vote. Swiss citizens may participate in the legislative process through optional and mandatory referendums and popular initiatives. The IPPAS team was informed that this can lead to the legislative process becoming quite complex, as any change in legislation that requires broad public involvement can lead to a referendum, all of which can take a long time.

The primary source of law in Switzerland is the federal laws. Constitutional rules (Federal Constitution) prevail over ordinary acts.

Pursuant to Article 90 and 118 of the Federal Constitution, the legislation on the use of nuclear energy and on protection against ionising radiation is enacted exclusively at the federal level. The authorities of the federation have therefore exclusive authority in establishing legislation in the area of the use of nuclear energy and in radiation protection.

Under the Federal Constitution, the legislative power is at the Confederation level vested in the two chambers of Parliament.

The legislative framework in the field of the peaceful use of nuclear energy and radiological protection consists of four levels:

- Federal Constitution,
- federal acts,
- ordinances (issued by the Federal Council or a federal department) and
- regulatory guidelines.

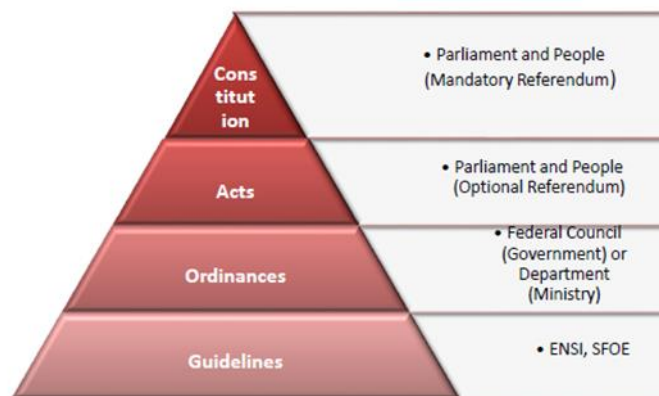


Figure 1. Legislative hierarchy

There have not been any substantial amendments to relevant legislation since the 2018 IPPAS mission, and specific changes are described in the relevant chapters of this report.

The main legal requirements concerning nuclear security are covered by the Nuclear Energy Act (NEA) and the Nuclear Energy Ordinance (NEO) (for more details see Chapter IV) and the main legal requirements concerning security of radioactive materials are covered by the Radiological Protection Act (RPA) and Radiological Protection Ordinance (RPO) (for more details see XIV.2).

III.2 Executive Branch

The executive branch in Switzerland is collectively represented by the Federal Council, consisting of seven members elected by the Federal Assembly. The Federal Council operates on collegial basis, with each member heading a specific department responsible for various policy areas such as finance, defence, foreign affairs etc. The President of the Swiss Confederation is elected annually from among the Federal Council members but the role is primarily ceremonial.

In the field of nuclear security numerous state authorities are entitled to administrate enumerated powers, as described below:

Federal Council serve as a licensing authority according to the NEA and issue general license to a nuclear facility. The Federal Council submits its rulings regarding the general licenses to the legislative branch, for approval. The decision of the Federal Assembly is subject to an optional referendum (public vote).

Federal Department of the Environment, Transport, Energy and Communications (DETEC) is the licensing authority responsible for the construction and operating license for nuclear facilities according to the NEA.

Swiss Federal Office of Energy (SFOE) under DETEC is the licensing authority according to the NEA (licenses for the handling of nuclear material and radioactive waste, including transport and export and mediation of nuclear technology) and the Federal Act on the Control of Dual-Use Goods (export of nuclear goods) and also serves as a supervisory authority according to the Safeguards Ordinance.

Swiss Federal Nuclear Safety Inspectorate (ENSI) is an independent supervisory authority for nuclear safety and security of nuclear facilities and material and for other radioactive material in nuclear facilities and their shipments in or out of nuclear facilities. ENSI also serves as licensing authority for activities concerning other radioactive material in nuclear facilities and the import and export of other radioactive material to or from nuclear facilities according to the RPO. It is also responsible for ordering all measures necessary and appropriate to ensure nuclear safety and security and for issuing permits and preparing safety and security evaluation reports as the basis of decisions by the licensing authorities according to the NEA and NEO. The ENSI establishes security criteria and requirements through its guidelines.

Federal Office of Public Health (FOPH part of the FDHA) is the licensing authority for radioactive material according to the RPO. It serves as a supervisory and enforcement authority for radioactive material in the areas of medical and research facilities (in the case of enforcement also industry and trade) and is responsible for the monitoring of radioactivity in the environment.

Swiss National Accident Insurance Fund (SUVA) is an independent non-profit fund and authority which is, according to the RPO, responsible for the supervision of radioactive material in the area of industry and trade.

Federal Department of Defence, Civil Protection and Sport (DDPS) is in general responsible for information protection and vetting on national level.

Federal Intelligence Service (FIS) under DDPS is an intelligence service responsible for vetting at the international level. It is responsible for assessing the national and international threat situation and for sharing intelligence with the necessary authorities.

National Cybersecurity Centre (NCSC) (Formerly the “Federal IT Steering Unit FITSU”) is currently under the FDF but from 01 Jan 2024 will become Federal Office for Cyber Security (FOCS) under the DDPS.

Federal Office for Civil Protection (FOCP) under DDPS operates the Spiez Laboratory used for NBC protection and for nuclear forensic analysis and serves as a National Emergency Operations Centre.

Federal Office for Customs and Border Security (FOCBS) under FDF is responsible for detection of material out of regulatory control.

State Secretariat for Economic Affairs SECO (EAER) is a licensing authority for export, import and transit of goods according to the Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods.

Federal Department of Foreign Affairs (FDFA) is responsible for international cooperation including non-proliferation on nuclear weapons.

Federal Office of Police (Fedpol) under FDJP is responsible for investigation, for national and international police cooperation and support and protection of special objects and individuals.

Office of the Attorney General (OAG) is responsible for investigation and prosecution of enumerated felonies and misdemeanours in the NEA and RPA.

Police (Cantons) serves as a public security force, response force at nuclear facilities, conducts investigation and enforcement and has a Special Weapons and Tactics (SWAT) team capability. Cantonal police in Aargau and also Solothurn have particular responsibilities for nuclear security.

The Federal Nuclear Safety Commission (established according to Article 71 of the NEA) performs advisory tasks on behalf of the ENSI, the DETEC and the Federal Council, including examination of fundamental issues concerning nuclear safety, participation in legislative work in the field of nuclear safety and reports on the ENSI's expert opinions. The establishment of the Federal Nuclear Safety Commission clearly shows the commitment of the Swiss Government to ensure the highest level of nuclear safety, by providing a second and independent opinion in nuclear safety relevant matters. During the previous 2018 IPPAS mission, it was recognised that the ENSI should consider establishing an advisory committee in the field of nuclear security. The IPPAS team was informed that there are insufficient national experts who are experienced in nuclear security in order to establish such a committee. A possible solution is to establish a committee of international experts but this solution is limited due to the sensitiveness of information connected to the nuclear security. Moreover, different stakeholders, including the competent authorities, regularly meet as members of the Group of Nuclear Partners. However, the GNP does not make formal decisions or issue official statements. The IPPAS team concludes the previous suggestion is closed but further encourage ENSI to identify a suitable body to provide over-arching advice and technical expertise in nuclear security matters.

III.3 Judicial Branch

The judicial branch is characterised by its independence from the other branches of state power and also follows the federal structure. The Federal Supreme Court is the highest court and oversees the application of federal law. The judicial branch also consists of cantonal and administrative courts. Judges are appointed by the Federal Assembly and ensure that the rule of law and protection of individual human rights within the whole federation is upheld. Courts play an important role in the legally binding interpretation of law, including nuclear law. Every licensing decision can be challenged in court (and subsequently appealed at the higher instance), with the exception of the general license where there are no rights to appeal. Moreover, the prosecution and adjudication of felonies and misdemeanours, in accordance with Articles 88 to 92 of the NEA, Article 43 and 43a of RPA and Article 226bis and 226ter of the Swiss Criminal Code, are subject to the jurisdiction of the Federal Criminal Court. As for the information in this chapter, there has been no change since the last IPPAS mission in 2018.

After comparing the punishable offences according to the Article 7 of the CPPNM/A with the provisions in the NEA and Swiss Criminal Code, it can be concluded that these provisions have been fully implemented into the Swiss national law. For comparison of these offences see following table:

CPPNM/A – Article 7	NEA, Swiss Criminal Code
a) unlawful handling	Article 89 para. 1 and 2 NEA, Article 226 ^{bis} par. 1 CC
b) theft or robbery	Article 139, 140 CC
c) embezzlement or fraud	Article 138, 146 CC
d) unlawful handling over boarders	Article 89 para. 1 NEA, Article 226 ^{bis} par. 2 CC
e) sabotage	Article 88 para. 1 a), b) NEA, Articles 226 ^{bis} par. 1, 228 and 230 CC
f) demand for NM by threat	Article 156, 181
g) threat to use NM or commit an offence	Article 180, 181 and 258 CC
h) attempt	Article 22 CC
i) participation	Article 25 and 26 CC
j) organization	Articles 24, 226 ^{ter} par. 1 and 3, 259, CC
k) contribution to the commission	Article 25, 26 and 226 ^{ter} para. 1 CC

Table 1: *Punishable offences – comparison of the Article 7 of the CPPNM/A and Swiss national legislation*

The IPPAS team was informed that based on Swiss legal principles, prosecution focuses on individuals, typically employees of a license holder, thus in general only individuals may be sentenced by the Swiss courts for felonies and misdemeanours. The Swiss legal framework does consider the prosecution of a licensee under exceptional conditions only, amongst others if felonies and misdemeanours cannot be attributed to a specific individual (Art. 102 Swiss Criminal Code). Thus, prosecution is mostly limited to individuals. Therefore, there is no effective administrative or criminal prosecution in place that could potentially result in sanctions for license holders (e.g., through fines) to enforce nuclear security legal requirements. Penalties imposed on the license holder are not an instrument of enforcement in the Swiss legal framework. The State should strongly consider establishing enforcement actions, including sanctions and/or administrative financial penalties (fines) to enhance compliance in cases where the operators fail to comply with security requirements established under the legislative and regulatory framework. This issue was raised in the IPPAS mission in 2018 (suggestion) and IRRS mission 2021 (recommendation). The IPPAS team believes that ENSI should make this action a priority and work in collaboration with other competent authorities to establish a graded approach for issuing sanctions related to security infractions.

III.4 Safety, Security and Safeguards in Switzerland

The NEA and particularly its Article 5, which came into force in 2005, introduced the basis for a comprehensive regulation that covers both nuclear safety and security. Both safety and security issues are addressed in the licensing procedures. From 2009, the ENSI is separated from the SFOE and since then the supervision of nuclear safety and nuclear security are united in a single authority. The responsibilities for oversight and enforcement of nuclear safety and nuclear security and in particular the liaison between safety and security are specified in the ENSI's management system. ENSI is the competent authority for both safety and security for nuclear materials and nuclear facilities and this is reflected also in its management system. ENSI is also responsible for radioactive materials that are used, and stored at nuclear facilities. For other radioactive materials refer to module 4.

The IPPAS team was informed that the interface between safety and security involves establishing regulatory guidelines, drafting safety reviews, issuing permits, inspecting the nuclear facilities and their modifications, evaluating notified events and performing emergency exercises while considering both aspects. On the other hand, the IPPAS team observed that although in practice the areas of nuclear safety and security are clearly distinguished, legislative requirements are sometimes formulated ambiguously.

Even though the concepts of nuclear safety and nuclear security aim to achieve the same objective, namely the protection of humans and the environment against the harmful effects of ionizing radiation, sometimes safety and security measures may be in contradiction. This was previously observed in the 2018 IPPAS mission. The IPPAS team was told that work related to security aspects needs to be strictly coordinated with the assessments that are performed by the ENSI from the safety point of view. Even though this interaction works in practice, there are no explicit provisions in the legislation (on statutory or ordinance level) which mentions that security measures should not compromise safety and safety measures should not compromise security.

Basis: NSS No. 27-G, para 3.2. states that “The State’s nuclear security regime should also provide for appropriate management of the interfaces between physical protection and nuclear material accounting and control and between physical protection and safety. The State has the responsibility to ensure that nuclear material accounting and control, safety and nuclear security requirements do not conflict with one another, and that these elements support one another as far as possible.”

Suggestion 1: The State should consider formalizing the management of the interfaces between safety and security in order to systematically identify potential conflicts and to ensure that nuclear security measures do not compromise nuclear safety and safety measures do not compromise nuclear security.

For Switzerland the responsible authority for safeguards is the Swiss Federal Office of Energy (SFOE) under the DETEC who serves as the supervisory authority according to Article 4 of the Safeguards Ordinance and is responsible for the implementation of the international safeguards commitments. NMAC for safeguard purposes is also under the responsibility of the SFOE at the state level. A national accounting system of all nuclear material under the international safeguards is maintained by SFOE.

The IPPAS team was informed that ENSI and SFOE have been discussing frequently on the interfaces between security and safeguards and that there is a working group meeting regularly on “3S” (safety, security and safeguards), where also FOPH and SUVA are present. However, the cooperation between ENSI and SFOE on NMAC has not been formalized through MoU or ToR. It is important that physical protection and NMAC provisions are considered in a coordinated and complementary manner to reinforce the defence in depth and to improve especially the detection of unauthorized removal of nuclear material, in particular protracted theft performed by insiders. As SFOE has a mandate and extensive knowledge regarding NMAC due to its mandate on safeguards, a formalized cooperation between ENSI and SFOE could significantly contribute to the nuclear security in Switzerland. Without formal and documented cooperation, a problem can arise if current ties are severed (e.g., by current workers retiring or moving on to other job) and experience from past negotiations and meetings is not passed on to the new employees. Even if, the IPPAS team did not find any evidence that cooperation is currently not working, the team considers that for preserving continuity, it would be worth to consider formalizing such cooperation e.g., in the form of MoU or ToR.

Basis: NSS No. 27-G, para 3.2. suggests: “The State’s nuclear security regime should also provide for appropriate management of the interfaces between physical protection and nuclear material accounting and control and between physical protection and safety. The State has the responsibility to ensure that

nuclear material accounting and control, safety and nuclear security requirements do not conflict with one another, and that these elements support one another as far as possible.”

Basis: NSS No. 25-G, para 2.5. suggests: “Both the State competent authority and the operator need to recognize the importance of using NMAC for nuclear security purposes. NMAC should be promoted within the nuclear security culture as an important contributor to nuclear security.”

Suggestion 2: The State should consider formalizing cooperation between ENSI and SFOE in order to improve the efficiency of the use of NMAC for nuclear security purposes.

It was recognized by the IPPAS team during the mission that the physical protection systems should be assisted by the nuclear material accountancy and control measures, in particular in facilities using bulk material, small items of nuclear material, or items from which it would be possible to recover small quantities of nuclear material without undue efforts. The PSI research infrastructures were mentioned as an example.

Basis: NSS No. 13, para 3.47. recommends: “Defence in depth should take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats.”

Basis: NSS No. 13, para 4.57. recommends: “The operator should ensure that any missing or stolen nuclear material is detected in a timely manner by means such as the system for nuclear material accountancy and control and the physical protection system (e.g., periodic inventories, inspections, access control searches, radiation detection screening).”

Basis: NSS No. 13, para 4.58. recommends: “The operator should confirm any missing or stolen nuclear material by means of a rapid emergency inventory as soon as possible within the time period specified by the State. A system for nuclear material accountancy and control should provide accurate information about the potentially missing nuclear material in the facility following a nuclear security event.”

Recommendation 1: ENSI should define NMAC objectives and provisions for nuclear security purposes to the attention of the licensees following a graded approach that would consider also the physical and chemical form of the nuclear material and the associated insider risks, in particular the risks associated to the protracted theft.

IV. LEGISLATIVE AND REGULATORY FRAMEWORK

IV.1 International Instruments

Swiss approach for international law is monistic which means that officially ratified and published international treaties becoming automatically part of Swiss national law. However, most of the international obligations in the field of nuclear security are not self-executive, which means that they need to be somehow implemented into the national legal framework or these international documents are not even legally binding at all (Nuclear Security Series).

Switzerland is a party to all of the most important international treaties in the field of nuclear law. Most importantly, Switzerland has been party to the original CPPNM since 1987 and, in 2008, also ratified its Amendment. The last IPPAS mission to Switzerland conducted a detailed review of Swiss legislation including the provisions in criminal law and extradition measures. In accordance with Article 14 of the

CPPNM/A, there is an obligation to inform the IAEA of its laws and regulations which give effect to the Convention. This notification was fulfilled in 2021.

Switzerland also made a political commitment with regard to the Code of Conduct on the Safety and Security of Radioactive Sources and to act in accordance with the Guidance on the Import and Export of Radioactive Sources.

Other international instruments relevant to nuclear security to which Switzerland is party are:

- International Convention for the Suppression of Acts of Nuclear Terrorism,
- Treaty on Non-Proliferation of Nuclear Weapons,
- Application of Safeguards in Connection with the Treaty on Non-Proliferation of Nuclear Weapons,
- Protocol Additional to the Agreement between Confederation and the IAEA for the Application of safeguards in connection with the Treaty on Non-Proliferation of Nuclear Weapons,
- Agreement Concerning the International Carriage of Dangerous Goods by Road.

Furthermore, Switzerland actively and regularly participates in international activities connected to nuclear security. For example, Switzerland served as a co-chair to The First Conference of the Amended Convention on the Physical Protection of Nuclear Material (2022) and currently participates in more than 50 international commissions of the IAEA, Nuclear Energy Agency, the Western European Nuclear Regulators' Association, the European Nuclear Security Regulator Association and other institutions with the aim of promoting nuclear safety and security. In addition, Swiss experts have taken part on various IPPAS missions worldwide. Based on this information, the IPPAS team concludes that Switzerland actively cooperates, consults, and exchanges information on nuclear security techniques and practices internationally. The IPPAS team also concludes that Switzerland has ratified all of the most significant international documents regarding the physical protection of nuclear materials and nuclear facilities and plays an exceptionally active role at an international level.

The NEA in article 104 explicitly authorizes the Federal Council to conclude bilateral international agreements concerning security and control measures for nuclear goods and radioactive waste. The IPPAS team was informed that Switzerland has signed bilateral agreements with all neighbouring countries for cooperation in nuclear safety and emergency preparedness matters and signed also some agreements with focus on security (e.g., agreement with Sweden from 2011 and USA from 1998).

The NEA in its Article 4 para 3 and Article 22 para 2 let. g as well as the NEO in its Article 25 para 2, Article 31 let. c require that regulated activities need to be conducted in accordance with experience and the state of art in science and technology and furthermore. According to Article 36 para 2 NEO, the license holder must monitor technological developments, including those relating to organizations and personnel, and must examine the extent to which conclusions may be drawn therefrom concerning the safety and security of the license holder's installation. Also, the DETEC is entitled to amend Annexes 2 and 6 of the NEO on the basis of recommendations from the IAEA.

According to the information provided to the IPPAS team, Switzerland has been a member of the IAEA Incident and Trafficking Database (ITDB) Program since its introduction. The SFOE (Point of Contact for Switzerland and also for Liechtenstein) is responsible for reporting into the ITDB based on the recently established procedure for coordination and national reporting. The ENSI and FOPH are also involved when incidents under its mandate are reported to the ITDB.

Considering the size and population of Switzerland and number of employees of ENSI and other regulatory bodies, IPPAS team observed that Swiss active international cooperation in the field of nuclear security is at a particularly high level. Bilateral cooperation e.g., with the Netherlands and

Germany, numerous participation on and hosting of IPPAS missions or presidency during the First CPPNM/A Review Conference might be highlighted in this regard. ENSI also according to the Article 2 para 3 Ordinance on the Swiss Federal Nuclear Safety Inspectorate host periodic review by external experts with regard to its compliance with the recommendations of the IAEA. ENSI set its goal which relies on continuous improvement of nuclear safety and security and the strengthening of nuclear supervision in Switzerland through active participation in the international regulatory exchange of information and experience.

Good Practice 1: ENSI regularly and actively participates in international events in the field of nuclear security and regularly invites international peer review missions for which it has undertaken as a commitment in legally binding documents in order to continuously improve nuclear safety and security and to strengthen nuclear supervision through active participation in the international regulatory exchange of information and experience.

IV.2 Laws and Secondary Legislation

IV.2.1 Laws

On the top of the Swiss hierarchy of law is the Constitution. This incorporates basic legal principles that are also applicable to nuclear security e.g., the principle of proportionality (every governmental action must be appropriate and necessary in order to achieve the targeted objective). The Constitution explicitly states that the legislative framework to ensure nuclear safety and radiation protection should be exclusively at the federal level (Article 90 and 118). Moreover, the Constitution enables the license holder to comment on the intended required measures (imposed by the regulatory body) according to the Article 29 para 2 of the Federal Constitution.

On the second level of the Swiss legal framework are federal laws. There are three main federal laws which are connected to nuclear security and the security of radioactive materials.

The Nuclear Energy Act of 21 March 2003, SR 732.1 (NEA) is the principal law establishing overall duties and responsibilities with regard to nuclear security of nuclear material and nuclear facilities. Its provisions cover essential elements of the legal and regulatory framework, such as the designation of the competent authority, provisions regarding the authority and powers of the supervisory authorities, their funding, the requirement for physical protection measures, the authorization regime, inspections and enforcement measures, including criminalization of acts directed against nuclear material and nuclear facilities.

The Radiological Protection Act of 22 March 1991, SR 814.50 (RPA) is a comprehensive body of legislation which regulates all activities, installations, events and situations that may involve an ionising radiation hazard (for more see Chapter XIV.2.1.).

The Swiss Federal Nuclear Safety Inspectorate Act of 22 June 2007, SR 732.2 (ENSI Act) establishes ENSI, the supervisory authority for nuclear safety and security, as an independent federal institution under public law.

The NEA is a special law in relation to the RPA which means if the NEA does not provide for a specific regulation the RPA also applies to the activities connected to the nuclear energy.

Since the 2018 IPPAS mission only a small number of amendments have been made to the NEA, such as modifications to the licensing process and criminal provisions. No changes have been made to the ENSI Act and therefore everything stated in 2018 IPPAS mission report is still valid.

A number of other acts cover specific aspects of legal nuclear security regime:

- The Intelligence Service Act of 25 September 2015, SR 121,

- The Information Security Act will come into force on 1 January 2024
- Swiss Criminal Code of 21 December 1937, SR 311.0,
- Government and Administration Organization Act, SR 172.010, etc.

It was observed by the IPPAS team that in Swiss laws, ordinances and various guidelines and other documentation the use of the terms ‘nuclear safety’ and ‘nuclear security’ is inconsistent. Therefore, the IPPAS team is convinced that the state should continue with ensuring that the terms “safety” and “security” are consistently distinguished in legal and other documents, e. g. there is explicitly mentioned safety and security in the Article 72 of the NEA but in case of safety culture safety is interpreted as both safety and security, the same in case of article 22 while speaking of general obligations on the part of the license holder. RPA even does not use the term “security” at all but article 31 is interpreted the way that it also covers security. It is important to highlight the necessity of having a clear legislation with consistent terminology. Current legal state of affairs and the fact that sometimes both terms “safety” and “security” are used and sometimes only term “safety” is used, may lead to the interpretation that when legislator do not use explicitly the term “security”, it was not intended to cover both safety and security. This has the potential for confusion both at the national and international level, could challenge effective management when planning and implementing different programmes and activities and may result to misinterpretation of these terms during the possible dispute or court trial. There is, therefore, the need for a common understanding and common terminology for these concepts.

The IPPAS team was informed that even though that general public might not understand entirely what is meant by the German term for “security” and especially what is the difference between this term and the term for “safety”, though it is possible to distinguish between these two terms in the legal documents – “Sicherheit” and “Sicherung”.

Basis: NSS No. 20, para 1.2. states: “Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that security measures do not compromise safety and safety measures do not compromise security.”

Suggestion 3: The State should consider continue ensuring that the terms “safety” and “security” are consistently distinguished in legal documents.

IV.2.2 Secondary legislation – ordinances

The third level of Swiss legislation is formed with ordinances. Ordinances always require a legal basis in a federal act, although this basis may be of a general nature. In the field of nuclear energy and radiation protection there are a number of relevant federal ordinances issued by the Federal Council or a Department (Ministry).

The Nuclear Energy Ordinance of 10 December 2004, SR 732.11 (NEO) contains detailed provisions regarding the applicable physical protection requirements as well as licensing procedures. This ordinance elaborates on the fundamental principles of nuclear safety and security, such as defence in depth, requirements on security, requirements for licenses (including for transport), reporting obligations of licensees, provisions on permits issued by the ENSI, quality management programmes, systematic security assessments, ageing management, modifications requiring a permit, and project documentation.

The Ordinance on the Organization of the Government and Administration is a general ordinance which serves as a legal basis for coordination and information sharing of the government and administration.

Other relevant ordinances in nuclear security include:

- Radiological Protection Ordinance of 26 April 2017, SR 814.501 (RPO) (see more in Chapter XIV.2.2.),
- Ordinance on the Swiss Federal Nuclear Safety Inspectorate (ENSI) of 12 November 2008, SR 732.21,
- Ordinance on Personal Security Background Checks of 4 March 2011, SR 120.4,
- Intelligence Service Ordinance of 16 August 2017, SR 121.1,
- Information Protection Ordinance of 4 July 2007, SR 510.411 (should be replaced by the new Information Security Ordinance in 2024),
- DETEC Ordinance on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials of 16 April 2008, SR 732.112.1,
- Safeguards Ordinance of 4 June 2021, SR 732.12,
- Ordinance on the Requirements for the Personnel of Nuclear Installations of 9 June 2006, SR 732.143.1,
- Ordinance on Security Guards of Nuclear Installations of 9 June 2006, SR 732.143.2,
- Ordinance on Personal Security Background Checks in the Area of Nuclear Installations of 9 June 2006, SR 732.143.3 (most probably will be replaced in 2024),
- Ordinance on the Requirements for the Personnel of Nuclear Installations of 9 June 2006, SR 732.143.1,
- Ordinance on the Transport of Dangerous Goods by Road of 29 November 2002, SR 741.621.

The IPPAS team acknowledges the work that has been done on the regulatory level regarding the cybersecurity of nuclear installations, especially by issuing the Guideline on Cyber Security in Nuclear Installations ENSI-G22/e. The IPPAS team has reviewed the contents of the ENSI-G22/e and concludes that it successfully addresses the suggestion from 2018 IPPAS Mission and establishes nuclear computer security regulatory requirements at a high level to ensure effective and measurable provisions consistent with the threat assessment and design basis threat. However, there is still a weak link to cybersecurity in the statutory level legally binding documents. Computer security or cybersecurity is not explicitly mentioned in the NEA nor the NEO and is not mentioned in the Basic Inspection Programme. The weakest link is in case of cybersecurity during transport. Guideline ENSI-G22/e is based on Article 10 para 2 and Article 12 para 3 of the NEO, Article 5 para 3 and Article 6 para 2 of the DETEC Ordinance of 16 April 2008 on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials and Article 70 para 1 letter a) of the NEA and these are only linked to the cybersecurity only through interpretation.

Basis: NSS No. 42-G, para 3.5. suggests: “The State should consider examples from other laws and international legal instruments (such as conventions) to assist it in defining computer security and its implementation as it relates to nuclear security.”

Basis: NSS No. 42-G, para 3.9. suggests: “The State should ensure that sufficient financial, human and technical resources are available to competent authorities for them to fulfil their responsibilities for

correctly interpreting and implementing their legal obligations relating to computer security in the State's nuclear security regime.”

Suggestion 4: The State should consider continuing to address cybersecurity in the legally binding documents on statutory and secondary legislation level in order to clearly define responsibilities of all involved entities for correctly interpreting and implementing their legal obligations related to computer security.

IV.2.3 Regulations and Technical Guidance

The Fourth level of Swiss legislation is comprised of guidelines. The ENSI, FOPH, SFOE and other authorities may issue guidelines which serve as support documents that formalize the implementation of legal requirements and facilitate uniformity of implementation practices. This is based on an explicit mandate in an ordinance or in its capacity as a regulatory body according to the jurisprudence. The IPPAS team was informed that the main difference between these two cases is that where there is specific provision in the act or ordinance, then the respective authority is obliged to develop and adopt a suitable guideline (e. g. Article 33 para 3 of the NEO stipulates that the ENSI shall specify the detailed requirements on systematic safety and security assessments in guidelines). Since guidelines are not binding from a strictly legal point of view, the license holders or applicants may choose alternative solutions. If they do so, they must demonstrate that their proposal is equivalent or provide a higher level of safety or security.

As adjudicated by the Swiss federal courts, administrative regulations are not considered to be legal norms; they cannot stipulate rights and obligations to private persons. Therefore, an enforcement authority cannot take supervisory measures based on administrative regulations, but has to base it on rules of law or an ordinance. Swiss federal courts also adjudicated that the adoption of administrative regulations is usually not regulated by law, but is in general considered admissible even without a special legal basis. The IPPAS team was informed and also observed that these guidelines usually describe in general the objectives, but not how to achieve these objectives, therefore, ENSI guidelines are mostly goal-oriented, whereas FOPH guidelines are mostly prescriptive.

ENSI has formalized its policy on regulations and guides in a new Mission Statement (adopted by the ENSI Board) in its management system. This statement contains five key Principles:

- ENSI's regulatory framework is harmonized with the relevant international requirements and is comprehensive,
- ENSI regulatory framework is based on existing, tried-and-tested regulations, insofar as they are suitable for application within its supervisory scope,
- ENSI issues its own guidelines only when it is necessary to do so,
- ENSI guidelines are drawn up transparently, with the involvement of all stakeholders (for classified guidelines the provisions of the Information Protection Ordinance apply and, therefore, there are limitations on transparency and public involvement),
- the degree of detail of ENSI regulatory framework is based on the hazard potential and the risk.

The IPPAS team was informed that according to the section 7.7 ENSI-process (ENSI internal directive – Basics of Supervision), those responsible for ENSI guidelines are responsible for reviewing the need to revise their guideline(s) at least once a year, taking into account changes in overriding law and relevant international operating experience (including informing the head of the Grundlagenkomitee promptly after an amendment to a law or ordinance comes into force) and for organizing a periodic full review of the guidelines by the specialists at least every 10 years.

Therefore, the IPPAS concludes that ENSI has sufficient provisions in order to keep their guidelines updated and in line with the current situations and most recent development in the international field.

The most important guidelines issued by the ENSI applicable to nuclear security are as follows:

- ENSI-A09 DBT for nuclear installations,
- ENSI-A10 Security barriers for nuclear installations,
- ENSI-A11 CCTV for nuclear installations,
- ENSI-B15 Security measures for the transport of nuclear materials and radioactive waste (new guideline from 2022),
- ENSI-B16 Deployment of external guards in nuclear installations,
- ENSI-G22 Computer security in nuclear installations (new guideline from 2019).

Moreover, the guideline ENSI-A12 (Technical systems for nuclear security in nuclear facilities) is currently in the draft stage.

At present these six guidelines developed by the ENSI are addressing particular topics of nuclear security. All-encompassing general guideline on nuclear security still does not exist but the IPPAS team was informed that it is in planned to adopt such a guideline in the future.

If appropriate, safety and security topics are integrated within the same guideline. The following guidelines have also elements applicable to nuclear security:

- ENSI-A04 Application documents for modifications to nuclear installations requiring a permit,
- ENSI-B02 Periodic reporting for nuclear installations,
- ENSI-B03 Reports for nuclear facilities,
- ENSI-B11 Emergency exercises,
- ENSI-G07 The organization of nuclear installations,
- ENSI-G09 Operational documentation,
- ENSI-G17 Decommissioning of nuclear installations.

Guidelines relating to the security of radioactive sources are addressed in the Chapter XII.2.2.

In line with the relevant recommendation provided by the IRRS mission in 2015, the IPPAS team also observed that the State should consider modifying the legal status of nuclear security requirements to ensure that they are legally binding per se in order to avoid the need to base their binding character on other circumstances (by issuing the binding order). The IPPAS team was informed that IRRS follow-up mission to Switzerland in 2015 covered this topic through its Recommendation but the IRRS mission report 2021 does not address this Recommendation anymore. Therefore, the IPPAS team considers also Suggestion 4 from the 2018 IPPAS Mission as closed. Nevertheless, the IPPAS team needs to underline that nuclear security requirements should be clearly addressed in the legally binding documents on the national level and this is particularly important as the main security needs and “requirements” are explained in the guidelines and not even in the general way in the NEO or the DETEC TA&SM ordinance. If the “requirements” does not have as basis the aforementioned articles, their values are even weaker. Therefore, IPPAS team is convinced that ENSI should consider strengthening the basis for their

regulatory guides and at the earliest possible opportunity will try to move the most important requirements into a fully legally binding document.

V. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

In Switzerland there are various authorities involved in the supervision of the activities connected to the peaceful utilization of nuclear energy and ionizing radiation. The federal legislation (NEA, NEO, RPA, RPO) defines the duties and responsibilities of the authorities having responsibilities for nuclear safety and nuclear security. Beside ENSI, responsibilities for the regulation of nuclear security are shared with many other authorities namely the Federal Council, the DETEC, the SFOE, NCSC, FOPH or FIS. CPPNM/A requires that each State Party shall establish or designate a competent authority or authorities responsible for the implementation of the legislative and regulatory framework. The IPPAS team in line with the conclusions of the 2018 IPPAS Mission asserts that the ENSI is considered as a competent authority, although some roles and responsibilities of a competent authority as described by the IAEA NSS recommendations are dedicated to the authorities mentioned above. Still, this situation is considered to be in line with the CPPNM/A requirements.

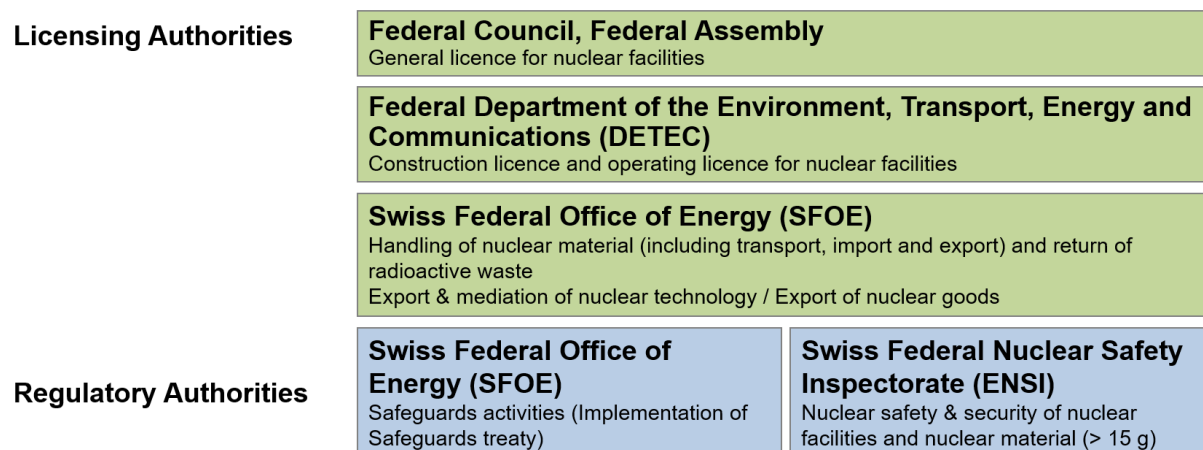


Figure 2: Main responsible authorities in nuclear safety and security

ENSI is the supervisory authority for nuclear safety and security. The ENSI Act establishes this authority as an institution under public law that carries out its supervisory work on safety and security (though this word is not clearly mentioned in the act) independently and autonomously. The main responsibilities are to monitor compliance with regulatory requirements and regulations, to order all measures necessary and appropriate to ensure nuclear safety and security, to prepare safety and security evaluation reports as the basis for the decision by the licensing authorities, to establish safety and security criteria and requirements that reflect experience and the state of science and technology and to grant permits. ENSI has also the statutory authority to participate in the preparation of legislation affecting its area of responsibilities, to represent the country in international institutions and committees and to directly communicate with the public.

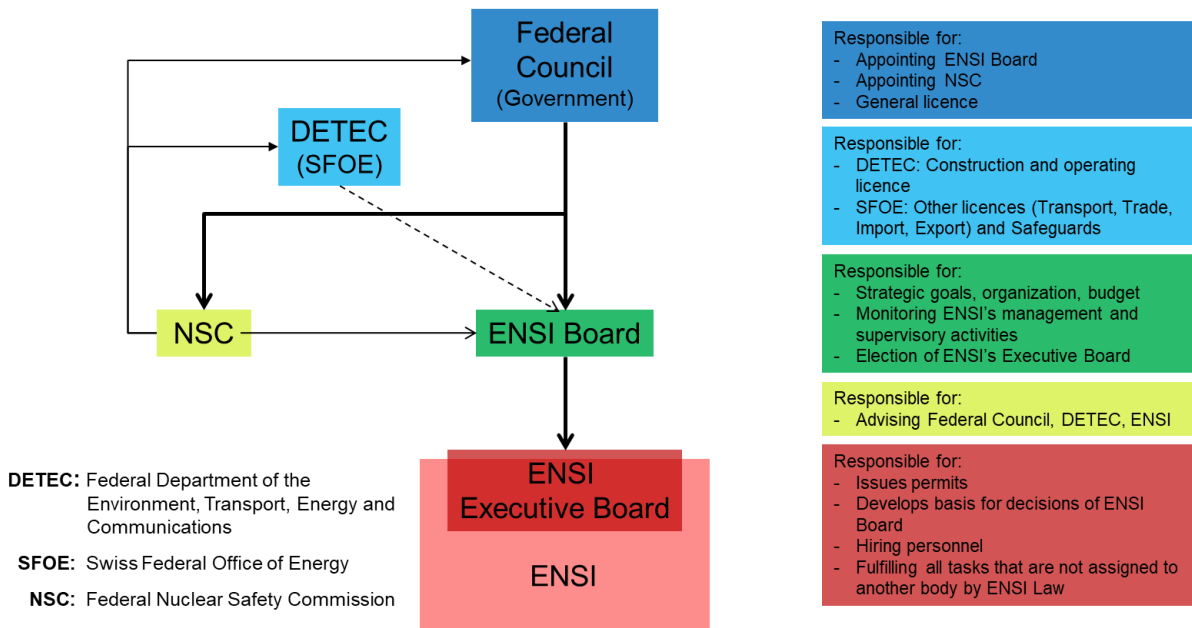


Figure 3: ENSI position in government, structure and responsibilities

Regarding its independence Article 70 of the NEA expressly states that the supervisory authorities according to this act are not bound on technical matters by directives, and must be formally separated from the licensing authorities. According to the Article 18 of the ENSI Act, ENSI performs its supervisory work autonomously and independently. This means that neither the Federal Council nor any other administrative authority is allowed to interfere in the supervisory activities of this authority. The IPPAS team was informed that the licensing authorities (Federal Council, DETEC or SFOE) base their decision on a safety evaluation report including security evaluations by ENSI and that even though there is no explicit requirement that obliges the licensing authorities to adopt conditions proposed by ENSI, in practice these proposals are always followed. Swiss federal courts adjudicated that the licensing authorities may and should base themselves on ENSI assessment unless there are valid grounds for not doing so. The public licensing process ensures that the licensing authorities consider ENSI assessment because the law requires them to be transparent and justify any deviation from ENSI suggested conditions.

These information leads in connection with financial independence of ENSI to the fact that ENSI might be considered as an independent competent authority according to the CPPNM/A. The IPPAS team was informed that currently ENSI has 170 collaborators with a budget of 65 million Swiss Francs. The section “Physical Protection and Cybersecurity” in the department of “Radioprotection” has currently 7 Full Time Equivalent (FTE) and in recent years added the field of cyber security to its main duties. This leads to the conclusion that Swiss competent authority is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities as it is required by the CPPNM/A.

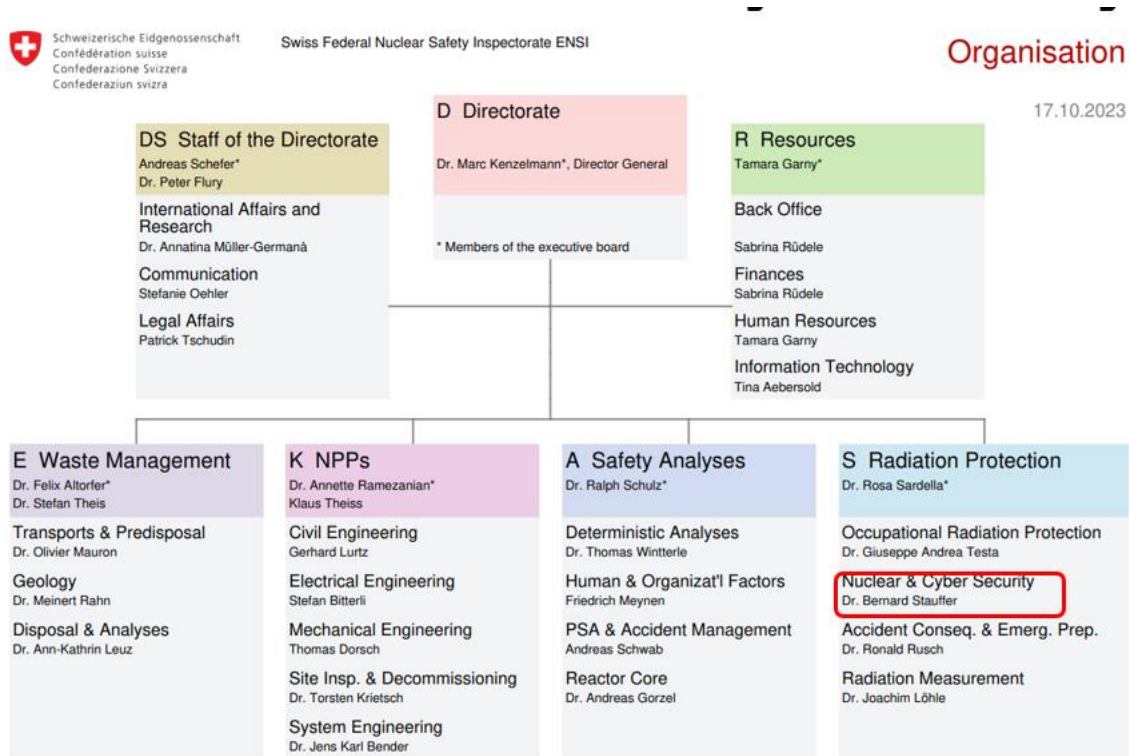


Figure 4: ENSI organizational structure

The Swiss Federal Office of Energy (SFOE) is the Swiss's competence centre for issues relating to energy supply and energy use at the Federal Department of the Environment, Transport, Energy and Communications (DETEC). Under the NEA, the NEO and the Safeguards Ordinance this authority is responsible for enumerated licensing activities and for safeguards.

Within the scope of the RPA, the responsibilities are allocated to FOPH (licensing authority and supervision of radioactive material in medical companies, research and training facilities), SUVA (supervision of radioactive material in industrial and commercial facilities) and ENSI (supervision of radioactive material in nuclear facilities with some licensing functions) – see more at the Chapter XIV.1.2.

V.1 Licensing/Authorization Process

Switzerland established its licensing process as it is required inter alia by the CPPNM/A and provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing and other procedures to grant authorization. The Swiss legislation on nuclear energy and radiation protection requires authorizations for all nuclear facilities, nuclear material and other radioactive material and related activities unless explicitly exempted on the basis of their risk (graded approach).

According to the NEA following activities require a license

- the initiation of a nuclear facility project,
- the construction and operation of a nuclear facility,

- the handling of nuclear materials, which specifically includes transport, import and export of nuclear materials,
- geological investigations to be carried out in order to closely examine potential sites for a deep geological repository,
- the deep drilling, shafts construction and carrying out explosions or other activities that affect a designated protection zone, defined as the underground area in which interventions could interfere with the safety of a deep geological repository,
- the change of purpose or scope of activities of a nuclear facility (amendment of the general license issued by the Federal Council),
- significant modifications of the original construction license, operating license, license for carrying out geological investigations (license amendments issued by DETEC),
- operator licenses for reactor operators and other staff in NPPs and research reactors.

According to the RPA following activities require license

- the handling of radioactive substances or equipment and articles containing radioactive substances,
- the manufacturing, distribution, installation or use of installations and equipment capable of emitting ionizing radiation.
- the application of ionizing radiation and radioactive substances to humans

The licensing process for nuclear installations and nuclear activities in Switzerland is based on the NEA. ENSI as a supervisory authority is directly involved in the licensing procedures (Article 73 of the NEO) and assesses the technical aspects of the license submission and subsequently, ENSI writes an expert opinion for the licensing authority (Federal Council, DETEC or SFOE). The primary task of the ENSI is to provide technical opinion of a semi-binding character and to license activities involving other radioactive material in nuclear facilities and import and export of other radioactive material to or from nuclear facilities, if not covered by the NEA license.

Authorizations in the field of nuclear energy and in relation to the use of ionizing radiation for nuclear energy are issued by several federal authorities, namely:

- **the Federal Council** who issues general license to nuclear facilities according to the Article 12 of the NEA,
- **the Federal Department of Environment, Transport, Energy and Communications (DETEC)** who issues construction license and operating license for nuclear facilities according to the Article 15 and 19 of the NEA,
- **the Swiss Federal Office of Energy (SFOE)** who issues licenses for handling of nuclear material (including transport, import and export), handling and return of radioactive waste and for export and mediation of nuclear technology according to the article 6 of the NEA and article 13 of the NEO. Also, it issues licenses for export of nuclear goods according to article 3 para 2 Goods Control Ordinance,

- **the Swiss Federal Nuclear Safety Inspectorate (ENSI)** who issues license for activities in connection to other radioactive material in nuclear facilities and import and export of other radioactive material to or from nuclear facilities according to the article 11 of the RPO, prepares safety and security evaluation reports as the basis for the decision by the licensing authorities and grant permits (authorisations for minor changes that are covered by a construction or operating license),

In the field of ionizing radiation for all other uses, authorizations are issued according to the RPA/RPO by:

- **the Federal Office of Public Health (FOPH)** who issues licenses for other radioactive material handling according to the article 11 of the RPO.

Conferring to the above list and according to the NEA there are four levels of authorizations

- licenses,
- orders (for the decommissioning of nuclear facilities and closure of deep geological repositories),
- permits and
- operator licenses.

The licensees' general responsibilities are listed in Articles 5 and 22 of the NEA and more detailed requirements are contained in the Article 28 and Annex 3 NEO. The IPPAS team was informed that when the NEA requires a license for certain activity, this license also covers all relevant radiation protection aspects and, therefore, no additional license under the RPA is required. This might be considered as something positive in terms of administrative burden imposed to the applicant. The IPPAS team was informed that where operation of a nuclear installation results in handling radioactive sources or devices emitting ionizing radiation that is not covered by the NEA license an additional license or permit is issued in accordance with the RPA. Licenses are issued for indefinite period of time except the license according to the RPA which are issued usually for 5 or 10 years period. In the Annex 4 of the NEO is listed the documentation for licenses and permits which must be submitted for the assessment of each application (e. g. security concept). The provisions for the evaluation of applications and orders, including physical protection, are described in Article 42 and following and 49 and following of the NEA.

The IPPAS team was informed that modifications of authorizations are issued by the same body that initially grants them and the procedure for amendments is mutatis mutandis the same as the procedure for granting. Basic conditions when general license may be granted are contained in the Article 13 of the NEA,

Regarding the modifications of licenses there are two different ways on how to approach them from the regulatory perspective. There are two different levels of authorization according to the NEA. These are licenses and permits. The activities and facilities that requires a permit are either defined in the nuclear legislation, or may be prescribed in the conditions attached to a license. Permits issued by the ENSI are inter alia required for amendments that do not deviate significantly from the relevant license, but which may have an influence on nuclear safety or security. The IPPAS team was informed that the licenses for operation of nuclear power plants are rather old and contain no special conditions regarding the nuclear security or even cybersecurity. In the text of NEA and NEO there are also only really vague criteria for

modifications that require a permit (and that do not deviate significantly from the respective license) regarding the security. Article 40 of NEO contains list of modifications that are generally regarded as modifications that do not deviate significantly from the respective license but which require a permit in accordance with Article 65 paragraph 3 of the NEA. This list contains many circumstances regarding the safety modifications which require permit. Compared to that, regarding the security there is one provision which stipulates that the modifications which requires permit are modifications to structures, systems and components subject to safety or security classification and to equipment relevant to safety or security. It is stipulated that these modifications can be made provided that the existing safety or security functions are maintained or improved. As the security classification is not defined, nor the explicit meaning of security function, it is not absolutely clear when modification affecting security requires change of a license or permit. This distinction must be made due to the fact that for modifications that constitute a significant deviation from the license, an amendment of the license is necessary and the corresponding procedure applies.

Basis: NSS No. 13, para 3.11. recommends: “The State’s legislation should provide for the comprehensive regulation of physical protection and include a licensing requirement or other procedures to grant authorization. The State should promulgate and review its regulations for the physical protection of nuclear material and nuclear facilities regularly. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership.”

Basis: NSS No. 13, para 3.12. recommends: “The State should license activities or grant authorization only when such activities comply with its physical protection regulations. The State should make provisions for a detailed examination, made by the State’s competent authority, of proposed physical protection measures in order to evaluate them for approval of these activities prior to licensing or granting authorization, and whenever a significant change takes place, to ensure continued compliance with physical protection regulations.”

Basis: NSS No. 13, para 3.27. recommends: “The *operator* should prepare a security plan as part of its application to obtain a license. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plans*. The *competent authority* should review and approve the security plan, the implementation of which should then be part of the license conditions. The *operator* should implement the approved security plan. The *operator* should review the security plan regularly to ensure it remains up to date with the current operating conditions and the *physical protection system*. The *operator* should submit an amendment to the security plan for prior approval by the *competent authority* before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The *competent authority* should verify the *operator’s* compliance with the security plan.”

Recommendation 2: The State should further clarify the conditions under which modifications affecting nuclear security require a permit or an amendment to the license.

Suggestion 5: Following Recommendation 2 above, ENSI should consider defining clearly the security classification and identify what SSC and equipment subject to this classification.

Regarding the operator licenses, they are granted for certain roles clearly identified in the Ordinance relating to the Qualifications of Personnel in Nuclear Installations (VAPK) by the holder of the operating license of the nuclear facility. This type of license can only be granted upon formal agreement of the ENSI when candidates pass the examinations specified in this ordinance.

V.2 Inspection and Enforcement

Continuous regulatory oversight ensure that the license holder fulfills its obligations in terms of safety and security. Once the license is issued, license holder must at all times maintain and sustain traceability of its documentation regarding the operation of the installation on the basis of records in accordance with Annex 3 of the NEO. For example, such documents are the Security reports which describe the current status of security measures in nuclear installation and Guard reports which contain the names of guard personnel and the duties to which they are assigned, plus details of routine controls, patrol activities, unusual observations and events, and contacts with external authorities. Articles 72 and 73 of the NEA empower ENSI to perform inspections. ENSI performs programmed (Basic Inspection Program for 10 years and Annual Inspection Programs) and reactive inspections as well as announced and unannounced inspections. The IPPAS team was informed that unannounced inspections have been carried out and they are part of the annual inspection planning. Each inspection has several stages:

- preparation of inspection report,
- announcement of inspection (depends on the type of the inspection),
- introductory discussion,
- fact-finding,
- preliminary evaluation,
- exit meeting (with possibility to comment on the results) and
- inspection report.

The regulatory body has established a process and has implemented a documented inspection programme (the documentation includes inspection guidance and procedures). The inspection process is supported by legal provisions conferring to the regulatory body all necessary authority. There is no general act on inspections in Switzerland but ENSI, FOPH and SUVA inspectors are entitled to conduct inspections and are endowed with vast powers and responsibilities according to the article 73 of the NEA and article 37 para 2 of the RPA and articles 187 and 188 of the RPO. According to these provisions, inspectors may also ask for engagement of third parties (e.g., experts or other companies) enter the private premises, request documents, collect materials, etc.

The IPPAS team was informed that the ENSI nuclear security inspection program is a part of the ENSI safety inspection program. For the year 2022, the number of the nuclear security inspection was approximately 2,6 % of the total number of inspections carried out by ENSI and the number of nuclear security inspectors is around 9 % of total number of inspectors.

The findings of nuclear safety inspections are rated according to a systematic safety assessment in a scale of 11 levels of different safety significance. The IPPAS team was informed that the nuclear security findings are also rated, but only using the non-INES scale grades.

ENSI inspections are conducted by the full-time dedicated site inspectors or by part-time dedicated facility inspectors. The IPPAS team was informed that the ENSI site inspectors are dedicated only for nuclear safety and not for security. Site inspectors are not even trained on the basics of nuclear security. Although, the IPPAS team was informed that due to the fact that all supervised nuclear facilities are in close vicinity to ENSI headquarters and therefore, ENSI nuclear security inspectors may inspect all possible discrepancies effectively and in a timely manner, IPPAS team concludes that it is important

that even site inspectors are at least on a basic level trained in nuclear security (e.g. with checklist on basic security needs that must be fulfilled) in order to capture possible urgent situations that might be problematic regarding the nuclear security.

Basis: NSS No. 27-G, para “3.43. suggests: “The competent authority needs to ensure that its inspectors have the necessary qualifications, training and experience to carry out their roles. The competent authority may specify qualification and training requirements for inspectors.”

Suggestion 6: ENSI should consider developing and implementing basic security training program for site inspectors in order to include basic security considerations during their weekly on-site inspections.

Since the enactment of the guideline ENSI-G22 also inspections dedicated to the cybersecurity are conducted. As there was no transition period for this guideline, these inspections were adjusted to the situation that license holders gradually adapted. In fact, their systems were adapted progressively to these requirements in order to be in line with the guideline. While this guideline came into effect three years ago, ENSI might consider in the future defining time limits in order to clearly determine when the guideline needs to be fully met.

General licenses can be formally withdrawn by the Federal Council (article 67 of the NEA). In case of an objective situation that (if not hindered in its evolution) might lead with high probability to damage (immediate threat), the ENSI may impose immediate measures that deviate from the issued license or issue an order according to the Article 72 of the NEA. In particular ENSI may order an immediate plant shutdown and allow restarting only when the necessary corrective actions have been implemented by the license holder. The IPPAS team was informed that the fact ENSI is empowered to issue orders allows ENSI to effectively enforce provisions of the ENSI guidelines.

The IPPAS team was informed that in the past there were also penalties imposed for the unlawful entry and damaging property at nuclear facility. As it was described in the Chapter III.3. penalties imposed on the license holder are not an instrument of enforcement in the Swiss legal framework. The IPPAS team concludes that this might be a problem in connection with the fact that prime responsibility for nuclear safety and security lies on the license holder. The IPPAS team is persuaded that this is necessary in order to balance the enforcement measures (sanctions) between licensees and individual natural persons. IPPAS team was also informed that a possible change in this general approach for imposing penalties legal entities is being discussed at a governmental level and this issue may be settled in the future following a recommendation of the IRRS Mission 2021.

V.3 Coordination with Other State Organizations that Contribute to Nuclear Security

The ENSI is an independent supervisory authority tasked with most of the responsibilities attributed to the "Competent Authority" as understood in the IAEA framework. ENSI is the national regulatory body with responsibility for nuclear safety and security of the Swiss nuclear facilities. Supervision of ENSI covers the whole lifecycle of a facility and related activities with oversight over projecting, siting, designing, operation of a facility until its decommissioning and the (final) disposal of radioactive waste but as it was described in the previous chapters, federal legislation defines the duties and responsibilities of other authorities having responsibilities for nuclear safety and nuclear security. In addition, federal legislation contains various provisions in order to ensure coordination and cooperation among the authorities (e.g., obligation to provide administrative assistance or provisions to settle conflicts regarding jurisdiction in administrative proceedings). This basis for coordination and information

sharing of all authorities is grounded in Articles 14 and 15 of the Ordinance on the Organization of the Government and Administration.

An important instrument for coordination of complex licensing procedures affecting the responsibilities of many authorities which is present also during the licensing according to the NEA is the so-called “concentrated decision procedures”. In concentrated decision procedures the authority whose responsibility is primarily affected, acts as a “lead authority” and decides on all relevant aspects. The other authorities, that could usually claim jurisdiction, refrain from taking their own decisions. Instead, they submit their opinions to the lead authority that has to duly consider them. In line with this principle, the DETEC or ENSI act as the lead authority and they have to consider the opinions of the other authorities, especially of those responsible for environmental protection and land use, planning and construction.

A good example of practical coordination and cooperation on nuclear matters could be the Group of Nuclear Partners, including majority of the authorities mentioned above, which meets twice a year for mutual information and coordination purposes and discusses, inter alia, matters related to the CPPNM/A. A similar group, the Coordination meeting of competent authorities for transport of dangerous goods class 7, meets once a year.

In many areas regulated activities are oversighted by numerous organizations on both federal and cantonal levels. The whole system is based on cooperation and information sharing of all involved parties. The IPPAS team observed, that the communication and information exchanges between the stakeholders heavily relies on non-formalized processes and personal knowledge. Some examples can be provided: the cooperation between DETEC, SFOE and ENSI regarding the security-safeguard interfaces, the coordination of inspections and transfer of knowledges between and within FOPH and SUVA or the DBT development which was made by ENSI but involved also indirectly FIS. Therefore, all involved parties should consider to formally arrange the communication and information exchange between all stakeholders (in the form of MoU, ToR, joint plans etc.) in order to achieve a regular, comprehensible and formalized way to exchange information between all relevant stakeholders. This might be particularly important in case of departure of responsible employees when acquired bonds and principles of cooperation can be lost and forgotten.

Basis: NSS No. 13, para 3.8. recommends: “The State should clearly define and assign physical protection responsibilities within all levels of involved governmental entities including response forces and for operators and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State’s physical protection regime. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the operator.”

Recommendation 3: The competent authorities should formalize arrangements for the communication and exchange of information between relevant stakeholders with nuclear security responsibilities in order to achieve regular, comprehensible and formalized interaction.

VI. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)

NSS No. 13 recommends that as part of their national protective security regime States should 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/A Fundamental principle G, States should base their physical protection on their evaluation of the threat. NSS No. 13 also recommends that the Competent Authority should be provided with information from other State organizations regarding the present and foreseeable threats to nuclear security.

According to Article 6 of the Intelligence Service Act of 2015 the responsibility to provide the national threat assessment in Switzerland lies with the FIS. The FIS obtains information and intelligence from a wide range of sources and agencies, both nationally and internationally, and uses this as the basis for threat assessment. The role of the FIS is furthermore defined in Art. 7 of DETEC Ordinance 732.112.1 on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials of 16 April 2008 where it is stated that “The Swiss intelligence services provide the supervisory authority with the basic information for the threat assumptions”.

The threat assessment document is reviewed and updated regularly and disseminated to those relevant federal and local authorities who need it. The threat assessment document is of a general nature and addresses a wide range of potential threats and there is no specific threat assessment for the nuclear sector available for ENSI on which to form the basis of the DBT.

In Switzerland, the regulatory basis for the design basis threat for nuclear installation is given in DETEC Ordinance 732.112.1. There it is stated, that according to Art. 3 of the DETEC Ordinance 732.112.1 in combination with Art. 6 of the Nuclear Energy Ordinance ENSI is instructed to regulate the relevant threat assumptions with consideration of the categories of nuclear materials and the radiological consequences in a classified guideline.

- For physical protection, the DBT is defined in the guideline ENSI-A09 DBT for nuclear facilities, last updated in 2017. According to the information provided to the IPPAS team ENSI A-09 defines the attributes, characteristics and modus operandi of the assumed adversary in the main document and there is comprehensive list of available tools, means and weapons in the Annexes.
- For Cyber-Security, the DBT is given in Annex 2 of the guideline ENSI-G22 Cyber security for nuclear facilities from December 2019. Provisions regarding blended attacks involving both physical and cyber aspects are covered in the ENSI-A09.
- For Transport, the DBT is defined in Annex 3 of guideline ENSI-B15 Security measures in the transport of nuclear material and radioactive waste.

Taking into account these three aforementioned guidelines, the DBT landscape developed by ENSI provides a strong basis for the identification and assessments of threats for the security of nuclear material in accordance with NSS No. 20 and NSS No. 13. For non-nuclear radioactive material, the IPPAS team noted that there is no specific DBT/RTS in place (Chapter XV.4).

Yet, although DETEC Ordinance 732.112.1 (and NSS 10-G) states that also the potential radiological consequences of unauthorized acts should be taken into consideration while developing the DBT, the

IPPAS team was informed that there are no radiological criteria for such an assessment of unauthorized acts – especially sabotage (VII.2.3).

The IPPAS team was informed that the DBT is periodically reviewed every 3 years or upon relevant changes to the threat assessment. For that purpose, according to Art. 7 of DETEC Ordinance 732.112.1, the FIS keeps ENSI informed of any changes to the national threat assessment. The IPPAS team was informed that there is a regular information exchange between FIS and ENSI concerning new and evolving threats, and this information exchange is formalized. However, there is no formalized document regarding national threat assessment. To secure the long-term sustainability of the threat assessment and DBT development process and to ensure that the historical foundation for the DBT and the underpinning rationale is preserved the nuclear specific threat assessment should be documented.

Basis: NSS No. 10-G (Rev. 1) para 4.5 suggests: “Relevant expertise for identifying and assessing credible threats might exist in several organizations of a State, such as intelligence organizations (including security agencies), ministries of the interior and foreign affairs, computer security centres, law enforcement agencies, military services, the regulatory body for nuclear security and other relevant organizations. Such organizations will have staff who are familiar with the processes of collecting and analyzing information and skilled in making the necessary judgements. In addition, such organizations may have access to particular sources of information, including information from contacts with other States or regional or international organizations”.

Basis: NSS No. 10-G (Rev. 1) section 2.8 suggests: “The results of the national nuclear security threat assessment process are recorded in the national nuclear security threat assessment documentation”.

Suggestion 7: The State should consider providing written documentation of the national threat assessment for the competent authorities in order to develop a Design Basis Threat.

The IPPAS team noted that DETEC Ordinance 732.112.1 provides a solid legal basis for the information exchange between ENSI and FIS which ensures ENSI’s information access regarding threats in the physical domain. Yet, according to Art. 2 of the DETEC Ordinance 732.112.1 ENSI is responsible for the regulation of the complete set of threat assumptions for the nuclear sector which also covers cyber security. With respect to that, the IPPAS team observed that there are no formalized channels or legal basis for the information exchange between ENSI and the Federal Office for Cyber Security (FOCS) / NCSC.

Basis: NSS No. 10-G (Rev. 1) para 4.6 suggests: "The responsibilities of competent authorities might include the following:

- (a) Collecting and collating information on potential threats;
- (b) Analyzing available threat information to ensure its credibility;
- (c) Sharing relevant threat information with other competent authorities;
- (d) Coordinating with other competent authorities to determine the subset of credible threats that are relevant to nuclear security;
- (e) Cooperating in the threat assessment process, identifying potential adversaries and documenting the national nuclear security threat assessment; [...]"

Suggestion 8: ENSI and FOCS/NCSC should consider formalizing their mutual information exchange by implementing a MoU.

NSS No. 10-G, discusses on relevant threat information that it should include recent and historical security events. The recent technical and geostrategic developments show a significant progress regarding tools and equipment which could also be used within the context of unauthorized acts against nuclear installations. This refers especially to the topic of uncrewed vehicles, both Uncrewed Aerial Vehicle (UAV) and Uncrewed Underwater Vehicle (UUV). Potentially, these vehicles may be used as a means of surveillance, transportation or even as weapon.

Basis: NSS No. 10-G, para 5.12. suggests: “Information should be collected on recent and historical nuclear security events (including those involving computer security), if applicable.”

Suggestion 9: ENSI should consider evaluating evolving threats posed to Swiss nuclear installations by uncrewed vehicles.

VII. RISK INFORMED APPROACH

VII.1 Risk Management

NSS No. 13, para 3.41, states that the State should ensure that its physical protection regime is capable of establishing and maintaining the risk of unauthorised removal and sabotage at acceptable levels through risk management. This requires assessing the threat and the potential consequences of malicious acts, and then developing a legislative, regulatory and programmatic framework which ensures that appropriate effective physical protection measures are put in place. In Switzerland, in general, this framework exists. Yet, the IPPAS team observed that no quantitative radiological criteria for the assessment of the radiological consequences exists (see Recommendation 5 in module 1 chapter VII.2.3). Also, the team noted that there is not a direct prescriptive link between the category of nuclear material and the security barriers of annex 2 of the NEO (see VII.2.2.). A similar observation was made regarding the classification of nuclear sensitive information and the trustworthiness (see VIII.3.1. and VIII.3.2.).

At the operator level the NEA states that appropriate measures shall be adopted that contribute towards risk reduction. Considering observations made during the IPPAS Mission 2018 and 2023 the IPPAS team noted that, at this level, risk was managed in a number of ways, for example, through the application of robust physical protection measures, defence in depth, nuclear security culture and by the design of the nuclear facilities.

In the field of physical protection of nuclear material, the IPPAS team noted no mentionable changes regarding the risk informed approach compared to the IPPAS mission in 2018. In the field of Cyber Security, the guideline ENSI-G22 *Cyber Security in Nuclear Installations* sets basic requirements for the use of a risk informed approach in this field. The IPPAS team was further informed that more detailed procedures and guideline exist on the plant/operator level. Details are given in module 5.

For the security of other radioactive material, in particular radioactive sources, significant advancements regarding the risk informed approach were made, these are described in detail in section module 4.

VII.2 Graded Approach

VII.2.1 Definition of Nuclear Material, Nuclear Installation and Radioactive Wastes

While nuclear material is defined in article 3 of the NEA as ‘substances that can be used for obtaining energy by means of nuclear fission processes’, not all these materials are covered by the NEO (article 1). In particular, the IPPAS team was informed that special fissile material with a weight up to 15 grams is not covered by this ordinance. While ‘nuclear installation’ is also defined in article 3 of the NEA, the NEO does not apply for all nuclear installations, in particular, it does not apply to installations containing special fissile material that contain a total maximum of 150 grams of plutonium 239, uranium 233 or uranium 235 (article 2.1.c). The IPPAS team was informed that the definition of nuclear installation of the NEA is such that facilities used for the interim storage of radioactive wastes, as the Federal Interim Storage Facility of PSI, are considered as nuclear installations even if these wastes does not contain fissile isotopes. The NEA specifically mentions in article 2.1.c that this act applies to radioactive wastes that are generated in nuclear installations (including those not containing fissile material) and also to the wastes not arising as a result of the use of nuclear energy which have been deposited in the Federal Interim Storage Facility.

VII.2.2 Categorization

The categorization table is provided in Annex 2 of the NEO. The NEO mentions in article 9.2 that the provisions from Annex 2 also apply to radioactive wastes. The categorization table “Security of nuclear materials and radioactive waste” is very similar to the categorization table of IAEA NSS13. However, the IPPAS team observed that:

- The table does not consider the possibility to take into account the self-protecting factor when fuel enriched to 10 % uranium-235 or more, fuel made of uranium-233 or fuel made of plutonium is irradiated. This is considered a conservative decision.
- High level activity vitrified wastes are considered as Category II, whatever fissile material the wastes contain.
- Annex II does not contain any clear link between security zones B, C and D (defined in the same annex) and the category of the material.
- Title 2 of Annex II specifies information regarding the security of Category I to III material.

Regarding the risk of theft associated with nuclear material containing less than 15 grams of special fissile material, the IPPAS team observed that while this material cannot be considered as Category I, II or III, at least prudent management practices should be clearly applied. The IPPAS team added that for some circumstances this material should be subject to NMAC measures in order to cope with the risk of protracted theft. Also, as NEO provisions on nuclear installations (including licensing) do not apply to installations containing special fissile material that contain a total maximum of 150 grams of plutonium-239, uranium-233 or uranium-235 (article 2.1.c), the IPPAS team emphasized that there could be situation for which Category III nuclear material would be present in facilities not considered as nuclear installations, in accordance with the NEO. Clarification of the security related provisions to be applied should be made.

Basis: NSS No. 13. para 3.1. recommends: “The State’s physical protection regime is intended for all nuclear material in use and storage and during transport and for all nuclear facilities. The State should ensure the protection of nuclear material and nuclear facilities against unauthorized removal and against sabotage.”

Basis: NSS No. 13, para 4.5. recommends: “The primary factor in determining the physical protection measures against unauthorized removal is the nuclear material itself. Table 1 categorizes the different

types of nuclear material in terms of element, isotope, quantity and irradiation. This categorization is the basis for a graded approach for protection against unauthorized removal of nuclear material that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g., plutonium and uranium), isotopic composition (i.e., content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity.”

Basis: NSS No. 13, para 4.14. recommends: “Nuclear material should be used or stored within at least a limited access area.”

Basis: NSS No. 13, para 4.22. recommends: “Nuclear material should be used or stored within at least a protected area.”

Basis: NSS No. 13, para 4.37. recommends: “Nuclear material should be used or stored within an inner area. An inner area could also be a vital area.”

Basis: NSS No. 27-G, para 3.71. suggests: “To grade protection against the unauthorized removal of nuclear material for use in a nuclear explosive device, the category of the nuclear material, [...], reflects the relative difficulty of using that category of material to produce a nuclear explosive device. Category I nuclear material should be protected with the most stringent levels of physical protection; nuclear material below Category III need to be protected only in accordance with prudent management practice [...].”

Recommendation 4: The State should conduct an assessment of its categorization process against the A/CPPNM to ensure that a graded approach is applied in protection of all nuclear material, in any quantity, that could be used in a nuclear explosive device. Based on the assessment, the State should take appropriate actions.

VII.2.3 Risk of sabotage

The IPPAS team was informed that the URC is not yet defined (see Chapter II).

Regarding the identification of the vital areas, the IPPAS team noted that the guideline ENSI-A10 defines in which security zones different Structures, Systems and Components (SSC) must be located, however, there is not a structured definition of a vital area.

Basis: NSS No. 13, para 5.20. recommends: “Nuclear material in an amount which if dispersed could lead to high radiological consequences and a minimum set of equipment, systems or devices needed to prevent high radiological consequences, should be located within one or more vital areas, located inside a protected area.”

Basis: NSS No. 27-G, para 3.94. suggests: “The threshold of unacceptable radiological consequences may be set at a level corresponding to a relatively small release of radionuclides in a localized area within the nuclear facility. Targets with the potential to cause only these lesser consequences may require a correspondingly low level of protection. At the other extreme, targets for which sabotage could potentially result in a substantial radiological release significantly affecting the population and environment beyond the boundaries of the nuclear facility need the highest level of protection [...].”

Basis: NSS No. 27-G, para 3.95. suggests: “Therefore, the State should also define the threshold for high radiological consequences. If the potential radiological consequences of sabotage are assessed to be greater than or equal to the high radiological consequences threshold, vital areas need to be identified and protected (...).”

Basis: NSS No. 16, Title 2.2.1.1. suggests: “The first significant policy consideration is the explicit decision regarding unacceptable radiological consequences and high radiological consequences. Typically, these consequence levels would be defined in terms of an unacceptable dose level, unacceptable radioactive material release level or unacceptable plant state, such as core damage for an NPP. It should be noted that if HRCs are identical with those defined by the State in relation with nuclear safety considerations, the safety analyses performed for the facility could be used for VAI without significant modification [...]”

Recommendation 5: The State should develop and establish a graded approach for protection of nuclear material and systems, structures and components against sabotage based on radiological consequences.

VII.2.4 Interface between the NEA/NEO and the RPA/RPO

The IPPAS team understood from discussions held during the mission that (1) radioactive wastes which do not contain nuclear material, but were produced as a result of the use of nuclear energy, and (2) radioactive wastes which were not produced as a result of the use of nuclear energy, but were surrendered to the Federal Interim Storage Facility, must be secured under the NEA/NEO regime. However, the IPPAS team did not find any specific provision regarding the security of Low-Level Wastes and Intermediate Level Wastes which do not contain nuclear material and/or which were not produced as a result of the use of nuclear energy. The IPPAS team observed that article 99 of the RPO specifically targets the security of High Activity Sealed Sources (HASS) but not Category I to III radioactive material which is not a sealed source. However, article 3 paragraph 6 of the UraM allows the supervisory authority to require a security plan if the inventory of radioactive materials is more than 100'000 LA (summation rule applies). This allows to cover on the one hand high activity materials that are not sealed sources and on the other hand also to cover some Cat.4 material wherever $100'000 \text{ LA} < 1 \text{ D}$ (e.g., Am-241).

Basis: NSS No. 14, para 4.3. recommends: “Security requirements for radioactive material should be based on a graded approach, taking into account the principles of risk management, including such considerations as the level of threat and the relative attractiveness of the material for a malicious act leading to potential unacceptable radiological consequences (based on such factors as quantity, its physical and chemical properties, its mobility, and its availability and accessibility). Security requirements should be adapted depending on whether the radioactive material concerned is sealed source, unsealed source, disused sealed source or waste, and should cover transport.”

Basis: NSS No. 11-G, para 5.48. suggests: “In principle, security levels can be assigned to radioactive waste in the same manner as described in paras 5.30–5.32 for other radioactive material. However, several considerations may lead to adjustments in the assignment of security levels to radioactive waste.”

Basis: NSS No. 11-G, para 5.50. suggests: “In addition, the default security level may be reduced to reflect the lesser vulnerability of radioactive waste in certain storage or disposal locations. Depending on the State’s regulatory requirements and infrastructure, radioactive waste could be located in short term storage at an operator’s facility, in long term storage at a dedicated (centralized) storage facility or in a disposal facility. Within a disposal facility, radioactive waste could be located in either of two primary areas: an operations area that is actively receiving, sorting and emplacing the radioactive waste; or a disposal area where radioactive waste has been disposed of, such as a borehole.”

Basis: NSS No. 11-G, para 5.51. suggests: “Radioactive waste in short term storage at an operations facility, in long term storage at a dedicated (centralized) storage facility or in the operations area of a

disposal facility could be assigned to the same security level as other radioactive material of comparable activity.”

Suggestion 10: As a basis for the graded approach for protection against unauthorized removal and sabotage of Low Level Wastes and Intermediate Level Wastes which are not nuclear material, the State should consider defining clear links between categories of these radioactive wastes and the different security zones mentioned in Annex 2 of the NEO. The categorization of these wastes could be based on NSS No. 11-G.

VII.3 Defence in Depth

In accordance with the Nuclear Energy Act and Article 9 of the NEO the protection of nuclear installations and nuclear material against sabotage and unauthorised removal shall be based on the principle of defence in depth, which encompasses structural, technical, organizational, personnel and administrative measures.

The ENSI guidelines clarify the regulatory expectation that a combination of multiple layers of systems and measures must be utilised for nuclear security. Annex 2 to the NEO in combination with guideline ENSI-A10 Security barriers describes the different zones and barriers to archive defence in depth. In addition, the guideline explains in which security zone SSCs important for safety should be protected. Based on a graded approach, the defence in depth architecture is also applied at non-NPP nuclear facilities such as the Central Interim Storage Facility ZWILAG.

In addition, it was explained that details of the methods and requirements to store and protect sensitive information, in hardcopy or electronic form, throughout its lifecycle and based on its classification is described in the Information Protection Ordinance. However, the IPPAS noted that there is not a specific nuclear security graded approach for the nuclear security information (VIII.3.1 below).

NSS No. 13 recommends that physical protection should use a defence in depth approach utilizing several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his/her objectives. While the IPPAS team in general observed very solid structural protection methods (barriers), it also noted that there were no clear requirements regarding the staffing of the CAS and was further informed that there were no thorough assessment of the effects of an potential insider attack performed by a single, unaccompanied person inside the CAS.

Basis: NSS No. 27-G, para 4.58. suggests: “Evaluations should also include analysis of the vulnerability of the physical protection system to insider threats. Guidance for performing such evaluations is provided in Ref. [9]. For analysis purposes, insider threats may be categorized by whether they are passive (e.g., the gathering of sensitive information only) or active, and if they are active by whether or not the insiders are willing to use force against a target or person. Taking into account the threat assessment or design basis threat, the evaluation may include consideration of the possibility of an insider colluding with another insider or with external adversaries.”

Suggestion 11: ENSI should consider establishing requirements regarding the plant specific assessments of potential insider threats for security personal, especially for personnel in highly sensitive positions like the CAS.

In the field of physical protection of nuclear material, the IPPAS team noted no mentionable changes regarding the risk informed approach compared to the IPPAS mission in 2018. In the field of Cyber Security, the guideline ENSI-G22 Cyber Security in Nuclear Installations states that “Cyber security

must correspond to the concept of defence in depth” and sets basic requirements for the application of the defence in depth principle. Details are given in Module 5.

For the security of other radioactive material significant advancements regarding the application of the defence in depth principle were made.

During the NPP facility visit the IPPAS team was informed that dedicated explosive detection equipment was used infrequently and randomly within pre-determined timeframes as agreed with ENSI. Based on the information provided, the IPPAS team considers the number of tests to be inadequate.

Basis: NSS No. 8-G, para 4.62. suggests: “Measures for the detection of prohibited items include manual searches of personnel, packages and vehicles (both periodic and random); use of metal detectors, X ray machines and radiation detectors; and use of dogs or other types of detector for chemicals and explosives. These measures should take into account the specifics of the facility and the threats against which protection is required according to the threat assessment or DBT, if applicable.”

Basis: NSS No. 8-G, para 4.64. suggests: “The stringency of searches and the determination of locations where they will be carried out should be commensurate with the sensitivity of the area where the search was triggered and the proximity of the area to the target. Searches should be carried out near the areas where the search was triggered. Periodic and random searches should be used to further deter the unauthorized removal or sabotage of nuclear and radioactive material. Searches should also be performed during emergency evacuation conditions, including exercises.”

Suggestion 12: ENSI should consider conducting an analysis that would take into account risks associated to insiders using explosives in order to determine what could be the appropriate frequency of searches for explosives for both persons and vehicles.

VIII.SUSTAINING THE PHYSICAL PROTECTION REGIME

VIII.1 Security Culture

The IPPAS team was informed that ENSI, as the main regulatory body involved in nuclear security in Switzerland, places a strong emphasis on nuclear security culture. As nuclear safety and nuclear security share the same common basic goals, ENSI considers that security culture should be seen as part of the overall nuclear safety culture. According to ENSI, this strategy prevents silos between safety and security and better ensures that security culture needs and beliefs are correctly approached as, in ENSI’s opinion, nuclear safety and nuclear security should be considered as important elements of the overarching organizational culture.

The IPPAS team was told that, when dealing with nuclear safety and nuclear security cultures in Switzerland, the term safety is used with an extended meaning and is considered as including security. The team was informed that since the last mission the guideline ENSI-G07 “The Organization of Nuclear Installations” has been reviewed. ENSI mentioned that in the new version of the guideline, more emphasis was given to safety culture (understood as including security culture) and other generic topics closely related to safety culture, such as leadership, responsibility and organizational resilience. The statement that security culture is part of safety culture is not made in the guideline. However, ENSI mentioned that it is clearly made and explained in the ENSI report on Oversight Practice "Oversight of Safety Culture in Nuclear Installations" which was revised in 2016 to address this issue. The IPPAS

team was informed that a member of the “Nuclear and Cyber Security” section was involved in the ENSI-G07 revision. This guideline is seen as the basis for oversight of organizational issues for both nuclear safety and security and will be brought into force before the end of 2023. Also, ENSI explained the team some examples of initiatives on security culture made by various operators, such as posters, thematic awareness events and agreed principles to which all personnel have to adhere to while working in the NPPs.

The IPPAS team concludes that ENSI takes the importance of security culture seriously and is acting in order to ensure that basic security needs are understood at all the levels in the nuclear sector. However, while the IPPAS team recognizes that one single organizational culture could include considerations of both safety and security, it is their opinion that nuclear security culture could not be seen as part of nuclear safety culture, as these concepts do not cover the same definitions even if there are shared basic goals. The IPPAS team was of the opinion that the terminology and concepts regarding this matter should be in line with the international texts and standards. In this perspective also, the IPPAS team noted that in the legislative and regulatory framework, there are many occurrences for which it is clear that safety is not understood to include security considerations (e.g., in the NEA/NEO and in the document “Swiss Federal Nuclear Safety Inspectorate ENSI.CH – INDEPENDENT COMPREHENSIVE INFORMED). ENSI expressed the idea that including security culture within the safety culture is an accepted solution in Switzerland.

The IPPAS team mentioned that, when addressing the security culture, it would bring a strong added value to put more emphasize in the texts on key concepts like confidentiality, trustworthiness, the belief that a threat exists and that the associated consequences could be high.

Basis: NSS No. 7, para 2.4. suggests: “While both nuclear safety and nuclear security consider the risk of inadvertent human error, nuclear security places additional emphasis on deliberate acts that are intended to cause harm. Because security deals with deliberate acts, security culture requires different attitudes and behaviour, such as confidentiality of information and efforts to deter malicious acts, as compared with safety culture.”

Suggestion 13: ENSI should consider that when addressing the nuclear security culture topic, specific emphasis should be placed on confidentiality, trustworthiness, the belief that a threat exists and that the associated radiological consequences could be high.

The ENSI mentioned that no specific nuclear security culture inspections are performed in Switzerland but that it promotes nuclear security culture in many different ways. The IPPAS team mentioned that the daily work of ENSI on nuclear security (e.g., for the permits and the inspections) contributes to assess in a continuous way the security culture of the licensees. However, the team emphasized the added-value of inspections that specifically target nuclear security culture.

VIII.2 Quality Assurance

management system, which is certified according to ISO 9001:2015. This management system consists of 26 main processes as presented below.

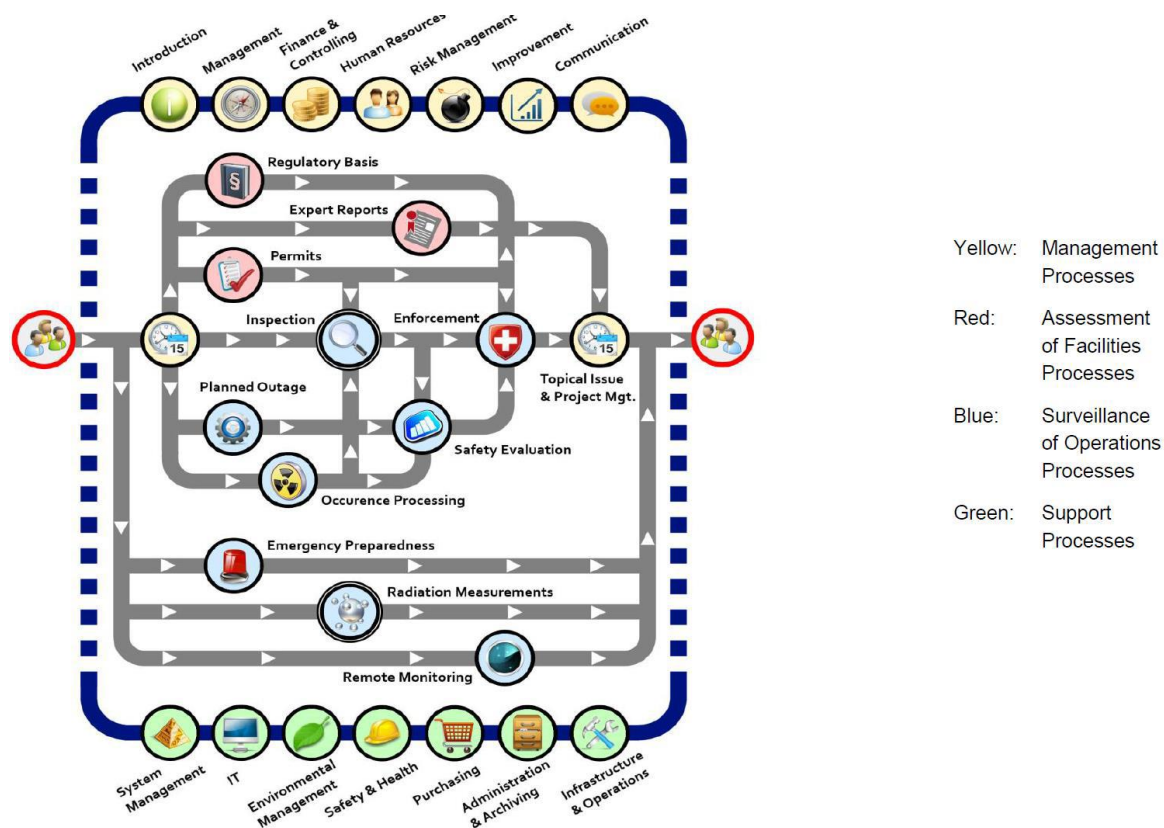


Figure 5: ENSI's management system

The processes regarding the nuclear security missions of ENSI are dealt with in the “Assessment of Facilities Processes” and the “Surveillance of Operations Processes”.

The entire documentation comprises around 800 single documents which include strategic documents, procedures and forms that are necessary for the conduct of the ENSI’s mission. It was also explained to the IPPAS team that easy, user-friendly access to the system documentation is provided by an electronic tool called “Squirrel”. The team was told that each of these documents is reviewed when necessary and on the basis of defined frequencies in accordance with the ISO 9001:2015 certification. Regarding the nuclear security responsibilities and missions of the ENSI, it was explained to the team that the documents of the management process support appropriately the “Nuclear and Cyber Security” section members. This topic was not further addressed during the IPPAS mission.

The IPPAS team noted that article 2.3 of the Ordinance on the Swiss Federal Nuclear Safety Inspectorate specifies regarding ENSI that: “It subjects itself to periodic review by external experts with regard to its compliance with the requirements of the International Atomic Energy Agency (IAEA)”.

VIII.3 Confidentiality and trustworthiness

VIII.3.1 Confidentiality

During the IPPAS mission, the team was informed that the legislative and regulatory framework for the classification and the protection of sensitive information is currently being reviewed, however, the team did not have the opportunity to gain more information on this ongoing process.

Regarding the current situation it was explained to the IPPAS team that currently the Ordinance on the Protection of Federal Information (Information Protection Ordinance, IPO) regulates the protection of federal information and that, in accordance with this ordinance, nuclear information could be classified and protected. It was mentioned that the classification scheme of the IPO is made following a very generic graded approach not targeting specifically nuclear security concepts. Since nuclear facilities are owned by private organizations, the obligations from the IPO to classify and to protect nuclear sensitive information at the licensee's level are not applicable. As a consequence, ENSI extended the provisions to classify information to the licensees in its regulatory guideline ENSI-G09 but it was not possible for the IPPAS team to assess to which level this guideline specifically stipulates security measures and/or objectives that should be followed, especially regarding the consultation, storage, reproduction, transmission and destruction of nuclear sensitive information. The IPPAS team understood from the provided explanations that there were two types of classification, one of them being supported by the ordinance whereas the other one is supported by an ENSI guideline. As an example, ENSI explained that information about nuclear security measures or cyber security measures is in general classified as confidential, whereas the DBT information is classified as secret. For sensitive information produced by the operators, the classification following ENSI-G09 does not have the same legal strength as the classification following the IPO.

While the IPPAS team does recognize the efforts made by ENSI to ensure that all nuclear sensitive information will be appropriately managed, it noted that there should be in place a coherent approach between the public and private entities, including the nuclear facilities and the companies which are involved in the transport of nuclear material. Also, the team emphasized the need to develop a clear classification scheme for the nuclear sensitive information that would be based on a graded approach associated to the risks of sabotage and theft of nuclear material. The IPPAS team emphasized the need to pay a specific attention to the holders of nuclear sensitive information which are not licensees (e.g., subcontractors).

Basis: NSS No. 23-G, para 3.1. suggests: “Securing sensitive information on a fragmented, facility by facility basis will not be effective. An effective national framework is necessary to ensure comprehensive security measures across all facilities, sites and organizations (governmental and non-governmental) handling sensitive information [...]”

Basis: NSS No. 23-G Para 3.9. suggests: “Detailed guidance on what constitutes sensitive information should be provided by the relevant competent authorities, in close liaison with the national security authorities and with the participation of users of nuclear material and other radioactive material [...]”

Basis: NSS No. 23-G, para 6.7. suggests: “Guidance on the classification to be applied to an information object should be provided by the relevant competent authorities in the form of a classification guide or guidance. Such a document groups information on particular topics and indicates the sensitivity of the information. Those who originate sensitive information should use such a guide when deciding on the appropriate classification level.”

Suggestion 14: The State should consider developing a coherent and consistent national policy regarding the security of nuclear sensitive information, in particular regarding the classification ranks and rules, across all facilities, sites and organizations (governmental and non-governmental) handling nuclear sensitive information.

VIII.3.2 Trustworthiness

While following the legislation and regulation generic provisions on information protection, persons having access to these should be subject to a background check in some circumstances, in addition to that article 24 of the NEA and the PSPVK set a clear and strong basis for the security background check in the area of nuclear installations. According to the PSPVK, persons having access (1) to information about nuclear installations and nuclear material that is classified as confidential or secret and (2) to classified information about safety or security relevant systems of nuclear installation or nuclear material, and (3) persons working in the nuclear security areas (as defined in annex 2 of the NEO) should be subject to security vetting procedures as described in the Ordinance on Personal Security Background Checks (PSPV). An exception exists for persons having short-term access to classified information about safety or security relevant systems of nuclear installations or nuclear material (article 5 PSPVK).

The IPPAS team were informed that three different levels of security background checks are defined: basic, extended and extended with personal assessment. Several registers and criminal prosecution records are checked during the security background process. While access to confidential information requires a basic background check, access to secret information is only allowed to people with an extended background check. The IPPAS team was informed that at ENSI, all the employees passed at least the basic background check while for the personnel having access to nuclear security information an extended background check is required.

In regards to the transportation of nuclear material transport, the IPPAS team was informed that in accordance with ENSI-B15 “the persons involved in the transportation with access to information classified as confidential or secret have a trustworthiness declaration based on the personnel security vetting. The trustworthiness of the other participants is ensured by appropriate checks”. Whilst this framework addresses the basic security needs in terms of trustworthiness. It does not provide clear trustworthiness provisions in respect of persons who have access to nuclear material or nuclear sensitive information outside nuclear installations. Indeed, regarding transports the aforementioned provision of ENSI-B15 does not specify what kind of personnel security vetting is necessary, also it is not clear what is meant by “The trustworthiness of the other participants is ensured by appropriate checks”. Also, the IPPAS team was not made aware of the existence of provisions applicable for people having access to nuclear sensitive information in premises located outside of nuclear installations. The fact that an important portion of nuclear sensitive information is classified but not following the IPO (VIII.3.1 above) is considered to be challenging. Also, the IPPAS team was not able to identify a graded approach for trustworthiness to be applied for access to security zones, to nuclear material and to nuclear sensitive information.

As a consequence, the IPPAS team observed that although there is a well-established trustworthiness regime there are areas to consider regarding the background check for persons working outside of federal entities who deal with nuclear sensitive information and nuclear facilities.

VIII.4 Sustainability Programme

It is considered, except for the suggestions 14 and 15 of the last IPPAS mission of 2018 (see Chapter II above), that the observations from mission 2018 are still valid.

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

IX.1 Contingency Planning at the National Level

NSS 20 Essential Element 11: Planning for, Preparedness for, and Response to, a Nuclear Security Event states that “a nuclear security regime ensures that relevant competent authorities and authorised persons are prepared to respond, and respond appropriately, at local, national, and international levels to nuclear security events”.

For public institutes the responsibility for civil protection and public safety lies with the individual cantons. Each canton has its own police act where the respective areas of responsibility are defined. For the canton of Aargau in which the NPPs Leibstadt and Beznau, as well as the Central Interim Storage Facility ZWILAG, are located, the police act (“Law on the guarantee of public safety”) states that the cantonal police are generally in charge – and in command – for all police operations in the canton, yet it may involve communal forces and forces from other cantons. Also, the civil part of the emergency response generally relies on the cantonal level and is guided by a cantonal command staff.

In addition to that, several organizations, such as the Federal Office for Civil Protection (FOCP), provide assistance at a state level. It develops specific guidance documents on how to deal with canton-overarching emergency situations, including a specific emergency concept for NPP accidents with underlying documentation to provide guidance for planning and performance measures.

The State’s duties are based on federal, cantonal and communal provisions which in turn are based on the Swiss constitution. These provisions ensure that the relevant organizations (predominantly ‘blue-light’ organizations) are prepared to deal with any kind of emergency. Nuclear security response strategies are developed by the State to manage escalation and restore control with the ultimate aim of returning the affected nuclear installation to a stable, safe and secure state.

In relation to regulated nuclear installations it is the responsibility of the licensee to implement emergency protection and security measures and responses to incidents, according to Article 5 of the NEA. In the case of malicious actions, it is only the police and guards who can use force against adversaries. The use of – potentially lethal – force by non-state guards leads to complex legal issues in many states. So, when a state considers the use of force by private guards as ultima ratio in the case of severe nuclear security events, it is advisable to give a solid legal basis including the applying conditions and limitations. The IPPAS team noted that Ordinance 732.143.2 on the *Security Guards of Nuclear Installations (VBWK)* provides this solid legal basis.

Good Practice 2: The rights and duties of the operator’s security guards in the case of nuclear security events are based on a precise, comprehensive and binding legal basis.

To support emergency response the state operates the National Emergency Operations Centre (NEOC) whose responsibilities include the coordination of the response to nuclear emergencies and the operation of the transport control centre during the transportation of nuclear material.

Regarding emergency preparedness in the context of severe accidents, the IPPAS team was informed by the command staff of the Kanton of Aargau that radiation protection equipment (e.g., dosimeters) is basically available, yet the quantities of this equipment may not be sufficient to deal with a severe nuclear accident.

The IPPAS team observed a force and force exercise at NPP Beznau, involving, among others, cantonal police, fire department, rescue services and also the cantonal SWAT Team (ARGUS). Based on the areas that the IPPAS team was able to observe, it appeared that the exercise was performed in a structured, well-organized way and all involved parties demonstrated a thorough dedication to their tasks and duties. However, the IPPAS team was also informed that this was the first exercise involving ARGUS for at least five years. It has to be noted that severe nuclear security events cannot be resolved by the operator alone, but requires assistance by state forces. IAEA NSS No. 37-G section 5.5 therefore suggests that regular exercises, involving all individuals and organizations with defined roles in the response to nuclear security events, are conducted. Thus, it may be considered to conduct exercises which also involve ARGUS more often.

The IPPAS team was informed that there are special provisions in case of a suspected attack on a NPP, a research reactor or an interim storage facility utilizing a (large) airplane, so called 'Renegade' scenarios. These provisions comprise fast communication procedures, measures of state forces including the Swiss Airforce as well as plant internal measures to mitigate the effects of such an attack and are exercised regularly.

Regulatory expectations are described in Chapter 7.7 of the Guideline ENSI-B11 *Emergency exercises* which largely relates to safety but also covers details of emergency response exercises involving the police.

The IPPAS team noted that there were well-developed relationships between the operators and cantonal police forces and the necessary arrangements to respond to a security incident in a timely and effective manner were in place. Co-ordination, enhanced by use of a common, encrypted communication system was seen to be very good, guards and police responders were well-trained and well-equipped; and agreed procedures and common, tactical language were in place. Response measures are exercised regularly on site, and lessons learned shared and procedures updated. Larger scale, multi-agency exercises involving other responders, the army and federal authorities are held less often. In addition, there are procedures and resources in place to locate, recover, and secure nuclear material and other radioactive material that is out of regulatory control.

Details of the operator's contingency plan is generally included in the security plan of the specific facility which is – with consent of the cantonal police – in general not routinely shared with the cantonal emergency organizations.

IX.2 Emergency and Contingency Planning Interface

NSS No. 37-G, para 1.4. suggests: "Both nuclear security events and nuclear or radiological emergencies should be considered. Furthermore, it states that nuclear security events connected with radiological emergencies may cause potential interagency conflicts which may result from a lack of understanding so it shall be ensured that the various response organizations have clearly defined and understood roles and responsibilities that are properly coordinated through the implementation of an effective multi-agency command, control and coordination structure."

As stated above ENSI-B11, which is the general guideline for the operator regarding emergency exercises, also covers nuclear security focused situations within a dedicated section and explicitly also mentions the interaction and information exchange of all involved organizations. One of the regular exercise goals is the "Compliance with a clear division of responsibilities between the plant's emergency organization and the cantonal police".

The IPPAS team noted, that the aspect “interfaces” is addressed in multiple ways and on multiple levels in the Swiss regulatory framework, both nuclear and non-nuclear.

TRANSPORT REVIEW (MODULE 3)

XII. TRANSPORT SECURITY LEGISLATION AND REGULATIONS

As it was more thoroughly described in the Chapter III.1 the legislative framework in the field of the peaceful use of nuclear energy and radiological protection consists of four levels. For transport security, the primary requirements are stipulated under the NEA and is regulated as part of the handling of nuclear material. As it was stated in Chapter IV.1 Switzerland is also a party to CPPNM/A and European Agreement Concerning the International Carriage of Dangerous Goods by road (ADR) which regulates the area of transport of nuclear materials.

Basic applicable provisions from NEA that are applicable for transport are related to the granting of a license and to the notification of events. Article 15 of NEO describes the documents which must be submitted for licensing the transportation of nuclear materials. According to Art 13 of the NEO, the licensing authority for handling nuclear material is the SFOE. The ENSI, as a supervisory authority for nuclear security, is also involved. Although security aspects are not directly mentioned the IPPAS team was informed that Article 15 para 2 let. g of the NEO requires evidence of compliance with the requirements on the carriage of dangerous goods and since Switzerland adopts the ADR for the carriage of dangerous goods on roads, the security plan and IAEA documents INFCIRC/274 and INFCIRC/225, mentioned in chapter 1.10 of the ADR, are indirectly referenced in the Swiss legislation.

In the second chapter of Annex 2 NEO, the basic requirements for the security of transport are described (Movement of nuclear material). Ordinance of 29 November 2002 on the Carriage of Dangerous Goods by Road also serves as a basic document regulating requirements for conducting the transport of dangerous goods.

Specific nuclear security requirements for all stakeholders are recently defined in the new Guideline – ‘Security Measures for Nuclear Material and Radioactive Waste in Transport’ (ENSI-B15) which supersedes former guideline (KE-R-13 of 2004) and details acceptable security measures with examples of transport configurations. This guideline is based on Article 3 paragraph 3, Article 5 paragraph 3 and Article 6 paragraph 2 of the DETEC Ordinance of 16 April 2008 on the Threat Assumptions and Security Measures for Nuclear Facilities and Nuclear Material (SR 732.112.1) and Article 70 paragraph 1 letter a) of the Nuclear Energy Act of 21 March 2003 (NEA; SR 732.1).

XIII. TRANSPORT SECURITY MANAGEMENT

The licensing process, the transport security requirements and the role of the cantonal police in transport activities were presented to the IPPAS team by ENSI. Since the last mission there have been many successful transports of different nuclear material types, including spent fuel, irradiated fuel rods and fresh fuel. The IPPAS team was, however, not in a position to witness the practical implementation of transport security arrangements.

The IPPAS team confirms that there remains a robust management system in place for transport activities that is based on the effective collaboration of the license holders (i.e., the consignor, the consignee, the carrier and the transport organizer), the cantonal police affected by the transport and the NEOC. The NEOC performs as the Transport Centre, based on a service agreement between the ENSI and the NEOC according to Article 8 of the DETEC Ordinance on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials (TA&SM). The NEOC has established a secure electronic platform (ELD) where all documents relevant to the transport are collected and stored. The ELD is accessible to all stakeholders prior to and during transport operations.



Figure 6: Nuclear Material Transport.

XIII.1 Threat and Target Identification

XIII.1.1 Allocation of Responsibilities

Article 15(1) of the NEA stipulates that the license application for the transport of nuclear material shall be submitted jointly by the consignor, the consignee, the carrier and the transport organizer. During the 2018 Mission the IPPAS team noticed that the legislation does not specify which organization has the prime responsibility for security out of the four stakeholders who shall submit a joint license application. It has been explained that ‘joint responsibility’ is a Swiss principle and therefore the relevant legislation will not be amended, however, there is now a requirement in the guideline ENSI-B15 that a single entity for the transport security plan should be designated. It remains the case that the cantonal police decide upon the necessary security measures needed during the transport based on their threat assessment and the category of the nuclear material. Although there is no legal requirement for the police to escort a transport, the IPPAS team was informed that in practice the transport of Category I and II nuclear materials are escorted by the police.

XIII.1.2 Transport Security Plan, including Contingency Plan

The IPPAS team observed during the 2018 Mission that there were no explicit regulatory requirements for the submission of a transport security plan for approval by ENSI prior shipment. The IPPAS team was informed that since the last Mission there is now a requirement for the submission of a transport security plan for approval by ENSI for the moves of Category I and II nuclear material (NM).

XIII.1.3 Interfaces with Nuclear Material Accounting and Control and Nuclear Safety

The interfaces with NMAC and nuclear safety are discussed in detail in Module 2. The advice provided there is also relevant for the security of nuclear material in transport.

XIII.1.4 Security Staff Training and Qualification

No change since the 2018 Mission.

XIII.1.5 Security Culture

Security culture in nuclear facilities is discussed in detail in Module 2.

XIII.1.6 Trustworthiness

The general findings as described in Module 1, also apply to transport operations. The PSPVK requires the background checks of persons only with security functions within nuclear facilities. However, ENSI-B15 now specifies that persons involved in the transportation of NM with access to information classified as CONFIDENTIAL or SECRET must have a trustworthiness declaration based on personnel security vetting. The trustworthiness of the other participants is ensured by appropriate checks; however, the content of the check is not specified and it is, therefore, unclear if the background of the drivers, who may pose relevant security risks as insiders, is effectively assessed. This matter is discussed in greater detail in Module 1 Section VIII.3.2.

XIII.1.7 Reporting of Nuclear Security Events

No change since the 2018 Mission.

XIII.1.8 System Evaluation, including Performance Testing

No change since the 2018 Mission.

XIII.1.9 Quality Assurance

The general assessment and findings as described in Module 2, also apply to transport operations.

XIII.1.10 Sustainability Programme

The general assessment and findings as described in Module 2, also apply to transport operations.

XIII.1.11 Confidentiality

No change since the 2018 Mission.

XIII.2 Transport Physical Protection System

XIII.2.1 Graded Protection and Defence in Depth

Following the 2018 Mission it was suggested that the ENSI should consider issuing a guideline on transport security requirements that is in compliance with NSS 13, taking into account NSS 26-G. During the 2023 Mission the IPPAS team was presented information showing that new guidelines have been introduced to cover transport security requirements (Guideline ENSI-B15 – ‘Security Measures In The Transport Of Nuclear Material And Radioactive Waste’). The guidelines apply to the transportation of Category I, II and III NM and radioactive waste and clearly set out the security requirements for all relevant stakeholders including responsible persons, escorting, application of the DBT and exercising.

XIII.2.2 Detection

No transport operations were observed during the IPPAS mission, thus the IPPAS team was not able to assess the detection measures for transport. The team was informed that the cantonal police are responsible for security of public areas and that in practice the Category I and II NM is escorted by the police.

XIII.2.3 Transport Control Centre

No change since the 2018 Mission.

XIII.2.4 Delay

No change since the 2018 Mission.

XIII.2.5 Response

No change since the 2018 Mission.

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

XIV. NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL

XIV.1 Assignment of Nuclear Security Responsibilities

XIV.1.1 State

Information provided in the chapters III - IX of this report regarding the legislative, executive and judicial process in relation to the physical protection of nuclear material and nuclear facilities is also applicable to the legislative and regulatory framework for the security of radioactive materials. Therefore, this information will not be repeated in this chapter. This module will focus on the relevant roles and responsibilities and the legislative and regulatory framework applicable for the security of radioactive materials, associated facilities and associated activities for the prevention of malicious acts.

In Switzerland, the State has the responsibility to establish, implement and maintain a national regulatory system of control for the safe and secure management of radioactive materials. Switzerland has an established and effective nuclear security regime that covers the safety and security of radioactive materials, associated facilities and associated activities. There are several competent authorities that have nuclear security responsibilities for radioactive materials. The State assigns the responsibilities for safety and security in the Radiation Protect Act (RPA). The responsibilities for regulating radioactive materials are well defined and clearly established in the RPA and Radiological Protection Ordinance (RPO). There are several coordination and communication mechanisms that will be discussed in section XIV.1.3.

In the addition to the above-mentioned, Switzerland has made a political commitment to the IAEA Code of Conduct on the Safety and Security of Radioactive Sources and its supplementary guidance on the Import and Export of Radioactive Source and Guidance on the Management of Disused Radioactive Sources. Switzerland also nominated a point of contact for the purpose of facilitating the export and/or import of radioactive sources. See chapter XIV.9. for import and export of radioactive sources.

XIV.1.2 Regulatory body

Federal Office of Public Health (FOPH)

FOPH is the licensing authority for radioactive materials used in medicine, research and industry. Furthermore, the FOPH is the supervisory authority in medicine, public research and training facilities. There are two sections that review the safety and security measures: Radiotherapy and medical diagnostics and Research facilities and nuclear medicine, presented in figure below.

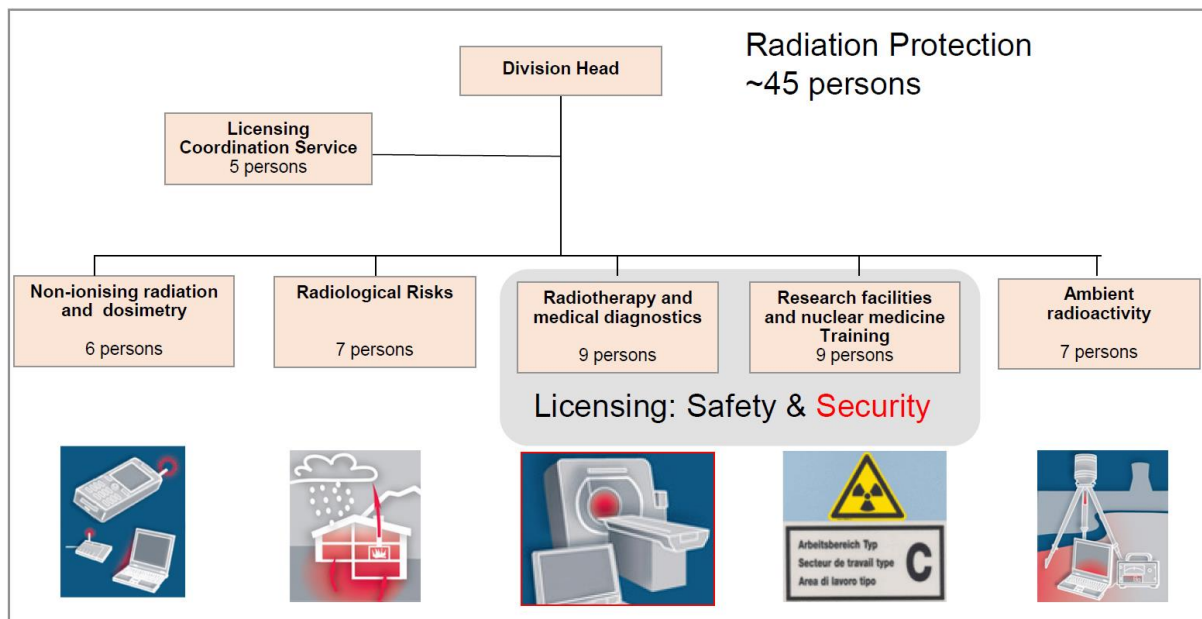


Figure 7: Radiation Protection Division at FOPH

Security of radioactive materials is a new task for FOPH inspectors. In 2018 and 2019, FOPH and SUVA inspectors were trained by a private firm to increase competence and build capacity. The new guideline for the security of HASS was published in 2019. During the implementation phase of the new guideline, the cooperation between ENSI and FOPH and FOPH and SUVA was increased to enable joint inspections and training for security inspections. In accordance with the Advance Information Package (AIP), FOPH plans to develop an internal training course on the subject of security. FOPH staff receive a two-week radiation safety course to become a radiation protection expert for radioactive materials. This includes sealed and unsealed sources. There are several training courses established that are specific to job position and requirements. The IPPAS team was told that there is a well-established inspector training program that includes continual education and refresher courses for safety. During the IPPAS mission, the IPPAS team noted that there is no formal security training course for inspectors who are responsible for the inspection of the security of radioactive materials under FOPH's mandate. A recommendation regarding training of inspectors for FOPH and SUVA can be found below.

FOPH established and maintains the Radiation Portal Switzerland (RPS). RPS contain information on all the license holders, including location, inventories and other licensing information. This will be further addressed in section XIV.2.5 National Registry and Inventory of Radioactive Sources.

FOPH reviews security plans for HASS as part of the licensing process. Information from the license holders is provided via encrypted transfer through the FOPH portal. Sensitive information is rapidly removed from the FOPH server once it is received.

Swiss National Accident Insurance Fund (SUVA)

SUVA is the supervisory body for radiological protection in industrial applications and participates in the authorization process conducted by FOPH. The Radiation Protection Team is responsible for the review and inspection of safety and security measures for HASS, such as Non-Destructive Testing.

As part of the authorization process, SUVA reviews the security documentation and provides a recommendation to FOPH for the delivery of the license. SUVA personnel have access to RPS to verify information and work in close collaboration with FOPH during the licensing process. SUVA reviews

the operator's security plan and ensures that new license holders have undergone a criminal record background check according to the guideline "Security of high-activity radioactive material".

SUVA inspectors conduct inspection visits before issuing the license. The IPPAS team was told that SUVA inspectors conduct annual inspection of HASS including unannounced inspections. SUVA also deliver radiation protection course for licensees and other collaborators that handle high risk radioactive sources that is mandatory and part of the licensing basis.

During the IPPAS mission, the IPPAS team was told that SUVA was in the process of implementing a new training module for the security of radioactive materials into existing training for radiation safety for licensees in collaboration with FOPH. In addition, licensees with HASS use security encrypted emails to share information with SUVA inspectors.

The IPPAS team was told that training was delivered during the implementation phase of the RADISS Action Plan. The IPPAS team noted that there is currently no formalized security training for FOPH and SUVA inspectors.

Basis: IAEA CoC, para 10 states that : "Every State should ensure that adequate arrangements are in place for the appropriate training of the staff of its regulatory body, its law enforcement agencies and its emergency services organizations."

Recommendation 6: FOPH and SUVA should develop and implement a formalized training programme for inspectors on the security of radioactive materials as part of their learning management system to maintain the competence and to strengthen capacity building of personnel assigned to security functions.

During the IPPAS mission, the IPPAS team noted the absence of security policies at the FOPH and SUVA. Security is a new task for these competent authorities. The IPPAS team was told that "security" is part of safety. However, there was no evidence that the security of radioactive material to prevent malicious acts is part of the overall organizational policies or procedures in the management system.

Basis: NSS No. 20 para 3.12. (c) states that "A nuclear security regime ensures that each competent authority and authorized person and other organizations with nuclear security responsibilities contribute to the sustainability of the regime by: [...] Developing, fostering and maintaining a robust nuclear security culture".

Recommendation 7: FOPH and SUVA should continue promoting and implementing an over-arching nuclear security policy that recognizes that credible threats exists, and that preserving nuclear security of radioactive material is important. In addition, the competent authorities should consider promoting and supporting nuclear security culture for radioactive materials.

ENSI

ENSI is the licensing and supervisory authority for radioactive materials at nuclear installations, including for the import and export of radioactive materials from nuclear installations and for the transport of radioactive sources from and to nuclear installations. The supervisory authority for nuclear installations is ENSI. This is covered under section V. Figure below summarizes the responsibilities of these three authorities.

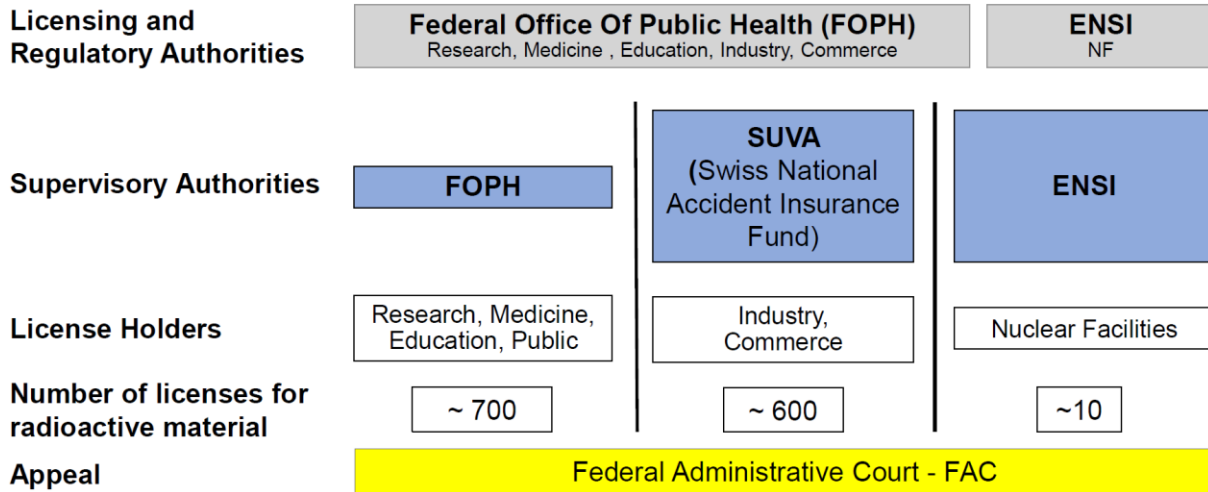


Figure 8: Nuclear security responsibilities for radioactive materials and associated facilities

XIV.1.3 Other Competent Authorities

FOPH works in close collaboration with several federal bodies. The FOPH and SUVA are the primary supervisory authorities (except for nuclear facilities) and interface with the Spiez Laboratory and the Federal Office for Customs and Border Security (FOCBS), as well as the Federal Intelligence Service (FIS), the National Emergency Operations Centre (NEOC), the Office of the Attorney General (OAG), the Federal Office of Police (Fedpol), the Swiss Federal Office of Energy (SFOE), the Swiss Federal Nuclear Safety Inspectorate (ENSI) and the Paul Scherrer Institute (PSI). The cantons (emergency services) also play an important role in response measures. Figure below shows the relationships between relevant organizations in the current RADISS Action Plan.

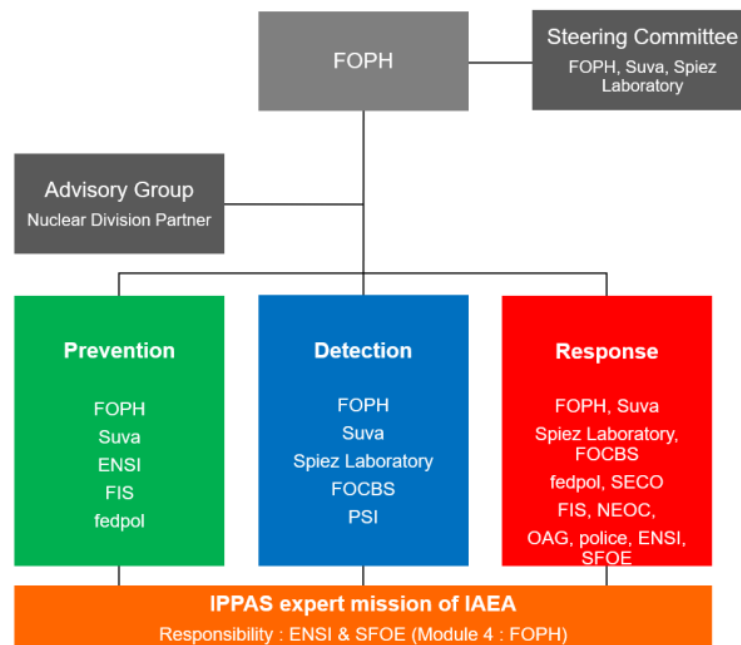


Figure 9: Organizational structure and relationships (Source: RADISS Action Plan)

Cooperation and coordination between competent authorities

The IPPAS team recognised that SUVA works in close collaboration with FOPH to ensure the security and safety of high-risk mobile radioactive sources.

During the IPPAS mission, the team observed that:

- FOPH and SUVA work in close collaboration for training inspectors in safety and security
- FOPH and SUVA share the same security requirements and guideline for HASS. They share the same internal guideline to protect sensitive information that is related to HASS.
- FOPH and SUVA conduct joint inspections and share experience and lessons learned on a regular basis

The IPPAS team found that FOPH and SUVA staff that are responsible for the review and inspection of the security measures for radioactive materials have established strong communication, information sharing and support mechanism. The IPPAS team encourages the two authorities to formalize their cooperation arrangements to maintain the current coordination and collaboration efforts and to strengthen their shared commitment to ensure the safety and security of radioactive material in the long term.

RADISS Action plan

In 2020, under the initiative of the FOPH, the Federal Council adopted an Action Plan 2020–2025 to strengthen radiological security and safety named “RADISS”. As part of the RADISS Action plan, several competent authorities have been engaged in projects to enhance the security of radioactive material. One of the main objectives of the action plan is to strengthen collaboration between federal departments involved in the response, and management of radiological events. There are three fields of action, eight priorities and 19 measures established in this strategy. These are described in figure below.




Field of Action	Priority	Measures
<p>Prevention</p> 	<p>P1: Strengthening the security of radioactive sources</p> <p>P2: Reduction of the number of high activity sealed sources</p> <p>P3: Gapless traceability of radioactive sources</p>	<p>M1: Implement international security standards</p> <p>M2: Ensure a sustainable quality of security</p> <p>M3: Establish a security culture through education and training</p> <p>M4: Promote alternative technologies</p> <p>M5: Examine and question the justification for the use of radioactive sources</p> <p>M6: Ensure data protection</p> <p>M7: Track sources from cradle to grave</p>
<p>Detection</p> 	<p>P4: Strengthening of monitoring in waste management and recycling companies</p> <p>P5: Ensuring and prioritizing checks for radioactivity at the border</p> <p>P6: Optimized use of existing measurement resources at federal level</p>	<p>M8: Seamless monitoring in affected recycling plants</p> <p>M9: Comply with international standards of measurement quality</p> <p>M10: Managing the correct disposal of radioactive waste</p> <p>M11: Risk-based monitoring concept for the import, export and transit of goods and on the entry of persons</p> <p>M12: Coordinated and targeted use of measuring teams</p> <p>M13: Ensure operational readiness in particular situations</p>
<p>Intervention</p> 	<p>P7: Ensuring efficient incident management through national coordination</p> <p>P8: Promotion of «lessons learned» culture through information exchange</p>	<p>M14: Clarification of responsibilities and procedures</p> <p>M15: Prompt and secure recovery of orphan sources</p> <p>M16: Minimization of damage in case of events</p> <p>M17: Consistent prosecution for illegal activities</p> <p>M18: Analyze and process events</p> <p>M19: Ensure international exchange</p>

Figure 10: Summary of the fields of action, priorities and measures of the RADISS 2020-2025 action plan

The IPPAS team considers that the various Swiss authorities with nuclear security responsibilities for radioactive sources are well established in the legislative and regulatory framework law. The IPPAS team encourage FOPH to establish and document written arrangements (such as terms of reference) or collaborative agreements with the relevant parties that are involved in the RADISS Action Plan working groups in order to formalize collaboration and strengthen long term commitment.

Good Practice 3: The IPPAS team commends the efforts lead by FOPH and compliment the outstanding collaboration and cooperation of the federal organizations that contributed to the success and accomplishment of the RADISS Action Plan. The active collaboration, coordination and cooperation among competent authorities will significantly enhance the safety and security of radioactive materials in Switzerland.

Good Practice 4: A national action plan has been established to enhance the safety and security of radioactive materials and involves representatives from the regulatory bodies, law enforcement, national security, criminal prosecution and intelligence community and other relevant organizations. The Action Plan contains a solid legal basis, strategy and three thematic areas with clear priorities and measurable objectives and timelines.

Basis: IAEA CoC, para 21 point a), b) and c) states that “Every state should ensure that its regulatory body is

- a) staffed by qualified personnel
- b) has the financial resources and the facilities and equipment necessary to undertake its functions in an effective manner.
- c) Is able to draw upon specialist resources and expertise from other relevant government agencies.”

Recommendation 8: The State should establish a long term plan to maintain the effective communication, collaboration and cooperation among competent authorities established under the RADISS Action plan and to ensure that sufficient resources are committed for secure use of radioactive materials at the national level and to sustain its nuclear security regime.

XIV.1.4 Operator, Shipper and/or Carrier

As part of the RPA and the regulatory framework, the operator, shipper or carrier is assigned the prime responsibility to implement and maintain safety and security measures to protect radioactive materials.

Overall, the IPPAS team found that nuclear security responsibilities are clearly defined and assigned in the current legal framework. Effective cooperation between the competent authorities is well-established and maintained. There are several mechanisms to share information among competent authorities.

Switzerland established a five years Action Plan (“RADISS”) to strengthen the safety and security of radioactive materials. The IPPAS team observed that the efforts and achievements resulting from this Action Plan have significantly enhanced the safety and security of radioactive material in the area of prevention, detection and intervention. In addition, the collaboration and cooperation between relevant parties has led to several positive outcomes that benefit the parties involved.

XIV.2 Legislative and Regulatory Framework

The legislative framework governing nuclear safety, radiation protection and nuclear security for radioactive materials is set out by the parliament in federal Acts. Regulations are enacted by the Federal Council or Departments in ordinances. The RPA and RPO provide the legal framework for radioactive sources facilities and activities. Figure below provides an overview of the relevant legislation for radioactive materials in Switzerland.

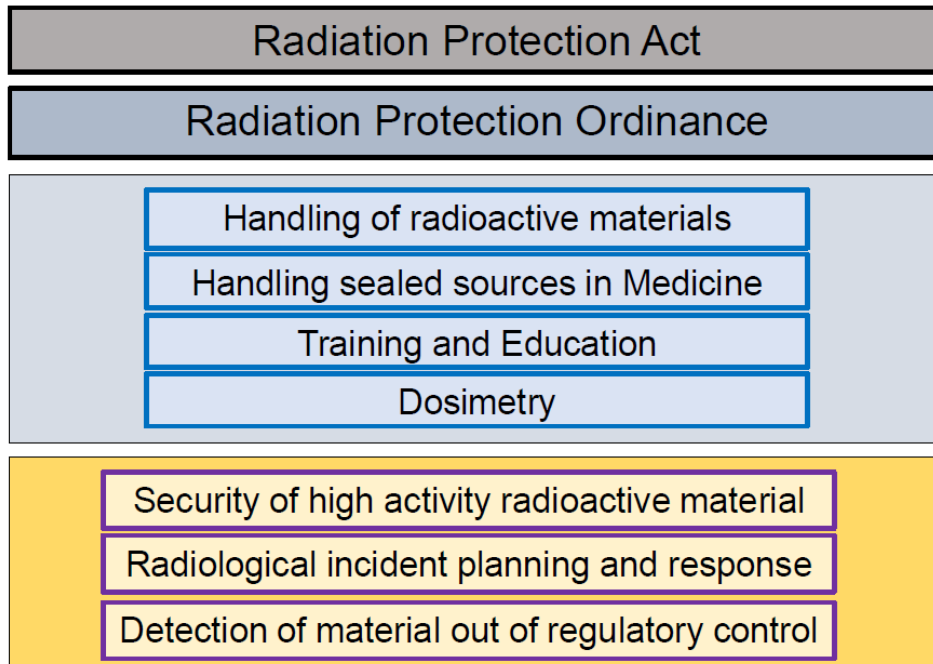


Figure 11: Legislative framework for radioactive materials

XIV.2.1 Laws

Radiological Protection Act (RPA)

The safety and security of radioactive materials is established by the Radiological Protection Act (RPA). The purpose of this Act is to protect people and the environment against the dangers of ionizing radiation. The RPA sets the general legal framework for the handling of radioactive materials. When it comes to the use of nuclear material, the NEA sets further specific requirements for nuclear facilities; at the same time NEA provisions on radiation protection, if any, take precedence on those of the RPA in relation to nuclear facilities. The RPA includes provisions for licensing, justification for benefits and license conditions. The RPA also include emergency actions and international cooperation considerations for any security events that involve radioactive materials.

Under the article 31, license holders are required to ensure the safe use of radiation sources. Although security is not explicitly mentioned in this article, the IPPAS team was informed that security is considered in these provisions.

In the field of nuclear energy, ENSI supervises radioactive materials at nuclear facilities. For other activities and facilities that handle radioactive materials, the licensing authority is FOPH. The supervision authorities and FOPH and SUVA is mentioned in sections V and XIV.1.2

Art. 8 of the RPA requires the licensee to justify the use of ionizing radiation device in terms of associated benefits and risks. In 2022, FOPH developed a new internal guideline for the justification of HASS. This guideline is used by FOPH and SUVA and describes the process and procedure for reviewing the justification for HASS. It includes an assessment of available alternative technologies that use non-radioactive sources, where available. The guide includes a risk index to establish a graded approach and considers the security risk related to the type of isotope, the quantities and the mobility factor.

The risk index $RI = \text{nuclear factor} \times \text{activity factor} \times \text{mobility factor}$

The intent is to phase out HASS when equivalent alternative technologies become available.

Good Practice 5: FOPH requires licensees to justify the use of ionizing source in terms of associated benefits and risk to society and have developed a comprehensive guideline for HASS justification. This document contains instructions on how to assess the application and includes security risk factors and a review of available alternative technologies. The objective is to phase out HASS when equivalent alternative technologies can be used, therefore permanently eliminating the risk related to HASS.

XIV.2.2 Ordinance

Radiological Protection Ordinance

Under the RPA, the Radiological Protection Ordinance (RPO) establishes the requirements to protect people and the environment against dangers from ionizing radiation. The RPO defines HASS and includes both safety and security provisions in article 99 that provides a risk-based, graded approach framework. These requirements apply throughout the entire lifecycle of the radioactive material from cradle to grave.

In accordance with article 99, every license holder shall define adequate (security) measures and procedures aimed at preventing unauthorized access to or loss or theft of the source.

The RPO provides the powers to FOPH as the licensing authority and includes requirements to report loss or theft of radioactive materials to the license holder. The RPO contains multiple requirements that apply for both safety and security, such as inventory control and training.

The RPO also includes other provisions that are relevant for security:

- Art. 101 to 103 contain transport requirements, including quality assurance verification, import, export and transit provisions,
- Art. 104 includes requirements for recycling and waste facilities to detect and search for MORC,
- Art. 135 includes provisions for the radiological protection strategy and national emergency response plan. It also mandates the FOCP to work with other competent authorities and the Cantons to prepare for national emergencies,
- Art. 190 mandates customs to verify the import, export and transit license for the transport of radioactive material.

In addition, the RPO contains provisions for coordination with other competent authorities for safety and security.

Ordinances on the Handling of Radioactive Materials (UraM)

This ordinance provides the basics conditions for the security of radioactive materials. UraM contains general requirements for the protection of HASS against theft and unauthorized exposure. It also includes requirements to protect sensitive information on the security of HASS. Art 3 includes specific provisions to prevent, detect, delay and respond to a nuclear security event.

The IPPAS team was informed that:

- The current Ordinance does not use the word sabotage but a similar term.
- Requirements for security functions and security managements are not explicitly mentioned in the ordinance. Requirements and guidance are established in a lower tiered FOPH guideline.

The current regulatory framework for the security of radioactive materials **could** be enhanced and the ordinances should explicitly mention the security objectives and requirements to solidify the regulatory basis and strengthen legally binding provisions.

Basis: IAEA CoC, para 18 point d) states: “Every State should have in place legislation and regulations that specify the requirements for the safety and security of radioactive sources and of the devices in which sources are incorporated.”

Basis: IAEA CoC, para 19 point g) and states: “Such legislation and/or regulations should provide for, in particular requirements for security measures to deter, detect and delay the unauthorized access to, or the theft, loss or unauthorized use or removal of radioactive sources during all stages of management”.

Basis: IAEA CoC, para 20 e) viii) states: ‘Every State should ensure that the regulatory body established by its legislation has the authority to measures to determine, as appropriate, the trustworthiness of individuals involved in the management of radioactive sources’.

Recommendation 9: The State should explicitly mention security of radioactive material at the appropriate regulatory level to provide clarity and consistency and establish requirements for the security of radioactive sources in alignment with the appropriate security guideline and ordinances.

XIV.2.3 FOPH Guideline

Security of high-activity radioactive material guideline

In 2019, the FOPH in collaboration with SUVA and ENSI developed requirements for the security of high-activity radioactive materials. This guideline expands on the requirements established under article 99 of the RPO and establish detailed security requirements and guidance on how to meet the security objective. The guideline is considered confidential and was revised in 2022.

The IPPAS team reviewed the guideline and found it to be very comprehensive; it includes guidance on how to protect sensitive information. The guideline includes a requirement for license holders to conduct their own security self-assessment on a regular basis. In addition, the guideline contains an annex that contains a detailed list of security questions that the license must answer for the purpose of self-assessment. The competent authority may request the licensee to provide this self-assessment for the purpose of enforcing compliance.

The security guideline also contains prescriptive requirements for the type of security barriers and intrusion detection systems. These measures must be installed by an accredited Swiss association security system installer. If the company is not accredited, the licensee must provide a proof that the IDS meet the certification criteria detailed in Annex 4.

Good Practice 6: The regulator requires HASS license holders to conduct regular self-assessment of their security measures and provide guidance and a detailed list of items to verify to meet this objective. This self-assessment may be reviewed by the regulator upon request.

The IPPAS team encourages FOPH and SUVA to enforce this new requirement in phase 2 of the RADISS Action Plan and share best practices with other license holders.

Good Practice 7: The regulator provides detailed intrusion detection system requirements and requires the certification of security system installers. These criteria are based on established industry security standards. Certified barriers must also be installed and meet certain resistance criteria. The barrier resistance classes include the intruder profile, tools required and break-in time. These requirements are

very clear for the regulator and licensees which makes them easy to review and accept during the licensing and supervision activities.

The IPPAS team identified the following areas of improvement to further align the guidelines with international guidance in IAEA NSS No. 11-G:

- Trustworthiness and reliability verifications should be extended for authorized individuals for security level B and C (category 2 and 3 radioactive source).
- Security plans should be labelled and identified as “sensitive information” in accordance with art 3 of UraM. The current “confidential” classification applies to government organizations and does not apply to private enterprises.
- Security of sensitive information should be addressed and guidance on how to protect electronic data and media should be introduced (refer to NSS No. 23-G). For the private sector, the coherency with the public sector should be ensured.
- Safety and security interfaces should be included in the HASS security guideline to ensure that safety and security measures do not contradict each other, during normal and emergency situations based on the guidance found in NSS No. 11-G.
- The frequency of inventory verifications should be clarified for the purpose of security and aligned with NSS No. 11-G. For example: daily verification to detect loss thought verification.
- Terminology for controlled area and supervised area should be aligned with RPO. The security zones should be linked to the security levels to provide clarity to avoid confusion between controlled area/supervised area and security area or temporary security area.
- The objective to provide immediate assessment of detection for security levels A to C should be clearly stated in the guideline to align with appendix II of NSS No. 11-G.
- For A and B security levels, the detection objectives should be considered to be aligned with NSS No. 11-G

Basis: NSS No. 11-G, para 6.38. suggests: “The regulatory body should require operators to limit unescorted access to.... individuals with a demonstrated need for such access in the performance of their jobs, whose trustworthiness has been verified [...]”

Basis: NSS No. 11-G, para 6.39. suggests: “[...] background checks could include disclosure of criminal conduct [...]”.

Basis: NSS No. 23-G, para 3.4. suggests: “The State’s relevant competent authorities should develop and issue policy and requirement specific to the security of sensitive information at nuclear and other radioactive material associated facilities and activities”.

Suggestion 15: FOPH, in collaboration with relevant competent authorities should consider revising the HASS security guideline to fully align with international guidance established in IAEA NSS 11-G (Rev-1), NSS 43-G and NSS 23-G.

FOPH reviews security plans and developed an internal checklist to review the information submitted by the licensee. This technical assessment is part of the licensing process and integrated in RPS. The licensee(s) must request access to RPS and use two factor authentication. Once the security plan is shared on RPS, it is quickly removed from the server to protect the information. Servers are hosted by FOITT.

The IPPAS team was informed that FOPH is currently developing a quality management system process. The IPPAS team encourages FOPH to establish and document its internal review process for security plans as part of its quality management system.

Monitoring of wastes and recyclable materials for radioactivity

As part of the RADISS Action plan, FOPH, in collaboration with relevant competent authorities and professional associations developed a guideline to facilitate the detection of radioactive material that may end up in waste management and/or recycling facilities. The guideline includes a requirement to detect and secure orphan radioactive material in a timely manner in order to protect the public and environment.

XIV.2.4 Trustworthiness verification

At the State level, SUVA and FOPH personnel undergo a trustworthiness verification by the government authorities as part of the on-boarding process. Vetting is conducted by the department of defence (DDPS). SUVA personnel and FOPH managers require a criminal record verification. However, the IPPAS team was informed that this requirement does not apply to FOPH personnel that have nuclear security responsibilities. There is a proposal to change the Personnel Security ordinance (PSPV) for FOPH personnel responsible for the safety and security of radioactive material licensing and supervision.

Basis: NSS No. 14, para 3.9. recommends: “The State should ensure that measures, consistent with national practices, are in place to ensure the trustworthiness of persons with authorized access to sensitive information or, as applicable, to radioactive material, associated facilities and associated activities.”

Recommendation 10: The State should ensure that FOPH personnel with security responsibilities for radioactive material with access to sensitive information or HASS undergo a trustworthiness verification that include a criminal background checks.

During the IPPAS self-assessment, FOPH identified the limited legal basis to perform extensive background checks on the applicant of a HASS license. The IPPAS team made an observation on the legal basis in XIV.2.1. Therefore, this will not be repeated in this section.

At the operator level, the FOPH requires trustworthiness and reliability verifications every five years, as described in the HASS security guideline. This includes for security level A criminal record verification and credit check. This requirement applies to individuals with access to confidential documents, sensitive information and unescorted access to radioactive materials. Escort provisions must be implemented for individuals that do not have a trustworthiness verification. It is the licensee’s responsibility to conduct these background checks. Figure below provides an overview of the requirements for each security level.

Figure 12: FOPH graded approach for trustworthiness assessment based on security level

The FOPH and SUVA inspectors review trustworthiness verification processes during inspections and it is also reviewed during the licensing process. The IPPAS team made an observation on trustworthiness verification for security level B and C in XIV.2.3.

XIV.2.5 National Registry and Inventory of Radioactive Sources

FOPH has established and maintain a national e-registry and inventory of category 1 to 5 radioactive sources on the Radiation Portal Switzerland (RPS). This also includes unsealed sources and other ionising radiation emitting devices. The new RPS is part of FOPH modernization plan to transition towards an E-government platform. The following table below provides an overview of category 1 to 3 HASS in Switzerland.

As mentioned in the AIP, there are approximately 1337 licensees for radioactive sources delivered to 513 different organizations. FOPH supervises 54% and SUVA 46% of these licenses.

Table 2: HASS used in the fields of medicine, industry and research as of January 2023.

In addition to the national register, licensees are required to maintain their own accounting records and conduct regular verifications and annual reporting to FOPH on RPS. Licensees are also required to update any changes and/or transfers online. The information on RPS is also shared with cantons, ENSI, SUVA and FIS. The IPPAS team was informed by FIS that this information is used to conduct security consultation visits at these locations to provide coaching and advice. These visits are not coordinated with FOPH.

Good Practice 8: FOPH has established a modern, online national e-registry for Category 1 to 5 sealed sources, unsealed sources and other ionizing radiation devices that is shared with other competent authorities, including the canton police forces, and security intelligence services to share relevant information and to coordinate security efforts.

XIV.3 International Cooperation and Assistance

The IPPAS Team was informed that as a member of the ITDB programme, SFOE (as designated Point of Contact) has represented Switzerland since 1995. In accordance with the national legal framework, several incidents have been voluntarily reported to the ITDB to exchange useful information. Switzerland's national security regime supports contributions to and voluntary participation in global security initiatives such as INFCIRC 901 and INFCIRC 908. The IPPAS Team was also informed that ENSI and FOPH actively participate in international and regional technical meetings, workshops, and training courses to gather and share information on lessons learned and implementation experiences regarding nuclear security.

The IPPAS Team was informed that, in accordance with Section 3, Art.23 of the RPA, there are bilateral agreements that exist between Switzerland and neighbouring countries regarding the exchange of information in relation to cross border nuclear safety related any events. Events are reported by ENSI and FOPH following the IAEA International Nuclear and Radiological Event Scale levels. In case of theft or sabotage of radioactive materials, the license holders must notify FOPH and FOPH may report this information to NEOC and FIS. At the international level, SFOE is responsible for gathering and analyzing events within the ITDB and disseminating the information to GNP. The IPPAS Team was informed that there is no formal procedure regarding the reporting of nuclear security events involving radioactive materials to the Federal Office of Customs and Border Security and other neighbouring States.

Basis: IAEA CoC, para 12. states: "Every State should ensure that information concerning any loss of control over radioactive sources, or any incidents, with potential transboundary effects involving radioactive sources, is provided promptly to potentially affected States through established IAEA or other mechanisms."

Basis: NSS No. 14, para 3.16. recommends: "For the purpose of reporting nuclear security events, States should consider establishing suitable arrangements to enable them to participate in relevant regional and international databases and international activities in accordance with their national legislation. One example is the IAEA's ITDB. Consideration should also be given to other bilateral and multilateral support arrangements."

Recommendation 11: The competent authorities should establish bilateral and multilateral agreements in case of loss of control of radioactive sources or any security incidents with potential transboundary effects.

XIV.4 Identification and Assessment of Threats

The IPPAS Team was informed that FIS is the responsible authority for gathering and processing threat assessment in accordance with Art.6 of the Intelligence Service Act of 2015. FIS is responsible for disseminating intelligence to other relevant authorities and this is performed mainly on a bilateral basis. FIS has the responsibility for conducting national threat assessment. The IPPAS team was informed that FIS has not assessed the national threat for radioactive materials. At the national level, there was no threat assessment or DBT used to establish security requirements for radioactive material, associated facilities and activities. As a result, there is no specific threat from DBT and/or Representative Threat Statements (RTS) that license holders may use as the basis for the design of their protective security measures.

SUVA best practice guide for the security of Non-Destructive Testing (NDT) provides examples of security measures in case of enhanced threat. The FOPH “Guideline Security of High Activity Radioactive Material” uses the IAEA security levels and categories and does not include provisions for threat assessments. The insider threat is addressed only in the “Guideline Security of High Activity Radioactive Material” which defines who may access material and confidential information. The IPPAS Team was informed that the FIS visit license holders of HASS to help them understand the consequences of insider threats and the importance of taking steps to protect the organization.

Basis: IAEA CoC, para 8 (f) states: “Every State should have in place an effective national legislative and regulatory system of control over the management and protection of radioactive sources. Such a system should: [...] provide for measures to reduce the likelihood of malicious acts, including sabotage, consistent with the threat defined by the State”

Basis: IAEA CoC, para 16 states: “Every State should define its domestic threat, and assess its vulnerability with respect to this threat for the variety of sources used within its territory, based on the potential for loss of control and malicious acts involving one or more radioactive sources.”

Basis: NSS No.14, para 3.17. recommends that “The State should assess its national threat for radioactive material, associated facilities and associated activities. The State should periodically review its national threat, and evaluate the implications of any changes in threat for the design or update of its nuclear security regime.”

Recommendation 12: The State should assess and periodically review the national threat and describe the motivations, intentions and capabilities of potential adversaries, including the threat of insiders to commit malicious acts to radioactive materials, associated facilities and associated activities and to inform relevant competent authorities. FOPH should use the results of the threat assessment as a common basis for determining security requirements for designing and evaluating of the security systems for radioactive materials, associated facilities and associated activities.

XIV.5 Risk Based Nuclear Security System and Measures

XIV.5.1 Risk Management

In accordance with Article 99 of the RPO, the Guideline on Security of High Activity Radioactive Material specifies in detail the structural, technical, and organizational security requirements applicable for category 1 to 3 HASS using a prescriptive approach. The guideline provides requirements based on the IAEA categorization and IAEA Security Level A to C as described in IAEA NSS No.11-G (Rev.1). The security requirements apply to radioactive materials in use, storage and transport. In accordance

with Art.3 of UraM and Art 96 of the RPO, HASS means a sealed radioactive source whose activity values are greater than the activity described in Annex 9. The table in annex 9 uses D values established in the IAEA publications. The guideline describes the security goals following a graded approach.

FOPH also requires a justification for using HASS with the intent of reducing the nuclear security risk associated with radioactive sources and encourages the use of non-radioactive technology. In accordance with the FOPH internal guideline “Justification of HASS”, the risk index (or threat index) is determined by evaluating the hazard and potential risk relating to the nuclide activity and other factors. The IPPAS team identified one good practice in XIV.2.3. The FOPH security guideline also describes the security requirements based on the defence in depth approach.

FOPH in collaboration with other competent authorities has encouraged the use of alternative technologies, such as X-ray irradiators to reduce potential risk related to HASS. As part of the RADISS Action Plan priorities, approximately 20 HASS have been removed for safe and secure disposal. The IPPAS team was informed that 90% cesium-137 have been removed since the beginning of this project. The last blood irradiator will be removed in 2024. The IPPAS commend the FOPH and their collaborators on achieving these results and permanently reducing the risk associated with these devices without any additional financial support.

Good Practice 9: FOPH and their collaborators have prioritized the replacement of blood irradiators with alternative technologies, therefore permanently reducing the associated risk of malicious acts.

XIV.5.2 Interface with the Safety System

SUVA and FOPH serve as the supervisory authorities to ensure the safety and security of radioactive materials (except for radioactive material in nuclear facilities where ENSI is the supervisory body for safety, security and radiation protection). The RPO Art.99 and UraM Art.3 clearly outline safety and security aspects. In line with this legal framework, the implementation of radiation safety and security measures are a prerequisite for obtaining a license for high activity sources. Coordination between FOPH, SUVA, and ENSI is defined by mutual agreement in the RPO Art. 184 para 5. Safety and security inspections were in some cases conducted jointly by FOPH and SUVA. Overall, the IPPAS team found that consultation and coordination interfaces are well maintained between the competent authorities regarding safety and security issues.

Security is a new task for FOPH and SUVA (the competent authorities) as, in the past, their primary focus was safety. Since 2018, significant efforts have been made to integrate security into the regulatory framework and inspection regime. Safety inspectors are gaining more experience in the area of security and the radiation protection team continues to build their competence. The IPPAS team found that the current interfaces between safety and security are robust and encourages FOPH and SUVA to continue strengthening these interfaces and integrate them into the organization management system, training and policies.

The IPPAS team also encourages FOPH and SUVA to make reference to safety and security interfaces in the security guideline and best practice guide to ensure that safety and security measures do not contradict each other, during normal and emergency situations and use the guidance in NSS No. 11-G. The IPPAS team made a suggestion to revise the guideline in XIV.2.3.

XIV.6 Sustaining the Nuclear Security Regime

Under the current legal framework, FOPH receives a budget from the state for the oversight of radioprotection and security of radioactive materials.

The IPPAS Team was informed that:

- The nuclear security regime for radioactive materials and associated facilities and the continued maintenance of measures following the conclusion of the RADISS Action Plan could not be sustained effectively for the long term due to FOPH’s limited human and financial resources,
- More resources are allocated to safety and radioprotection than nuclear security,
- Inspections regarding security have to be carried out in concert with the resources dedicated to safety,
- There is no dedicated security working group,
- FOPH security team comprises of only 2 persons,
- Every inspector in FOPH (radiation protection teams) received training from a private security company in 2018-2019.

The IPPAS Team was informed that:

- Every inspector in FOPH is a professional expert in radiation safety. However, there are no specific qualifications or training requirements for security inspectors,
- Every inspector in FOPH has a basic knowledge of security to perform security inspections. However, there is no specific, systematic training on the security of radioactive sources and formalized security training for inspectors is not delivered on a regular basis.

Basis: NSS No.14, para 3.29. recommends: “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 13: The State should ensure that FOPH has sufficient human and financial resources to develop and sustain competence, capacity and compliance activities to ensure the oversight of safety and security of radioactive materials.

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

The IPPAS Team was informed that the RPA Art.31 requires the license to ensure safe and secure operation. Art.125, 126 and 135 of the RPO refer to preparedness measures and the implementation of emergency preparedness. The legal framework puts the responsibility on the licensee to prepare for emergencies and to respond to nuclear security events. The FOPH security guideline for HASS requires licensees to respond to and report malicious acts to the competent authorities, as detailed in their security plan.

The IPPAS team was informed that there is good communication and coordination between federal and canton organizations to support the response to a nuclear security event at a nuclear facility. FOPH is leading the RADISS Action Plan to expand this good collaboration to include the response to radiological incidents.

As part of the RADISS Action Plan, coordination and cooperation between federal organizations has been enhanced to strengthen the exchange of information and optimize available resources. A dedicated working group was established to examine Response. This working group includes representatives from

FOPH, SUVA, FOCP, NEOC, FOCBS, Spiez Lab, SFOE, ENSI, Fedpol, FIS, OAG and the Swiss Army. As part of RADISS, the FOPH, in collaboration with other competent authorities, developed guidance on radiological incident planning and response to facilitate the intervention and collaboration between authorities and special units. The IPPAS team found that the new guideline provides very clear instructions and recommendations on the response to a radiological incident, including detailed instructions and a decision flow chart for different types of security scenario.

The IPPAS team was informed that during phase 2 the RADISS Action Plan there will be more liaison with cantonal police forces, together with joint exercises to test, assess and enhance the response to a radiological incident, which do not result in national emergencies (out of scope of RADISS Action Plan).

The IPPAS team was informed that:

- The RADISS Action plan covers incidents that can be handled by the competent authorities and are not national emergencies.
- The licensee is required to report security events to FOPH and SUVA when applicable.
- In their security plans, license holders of HASS must describe the requirement to inform the cantonal police of security events. Licensees must also inform the cantonal fire department regarding locations, types and activity of radioactive material.
- The cantonal polices have access rights to the national registry system for HASS which is operated by FOPH. The cantonal polices can view the inventory, location and relevant license holders' contact information within their areas of responsibility.
- The IPPAS team was informed that there is a draft national response plan for nuclear and radiological emergencies. This gap was already identified the first time in the IRRS Mission 2011, and then again in the IRRS 2021 mission to Switzerland. Consequently, there is no specific national response plan for a radiological emergency stemming from a malicious act with radioactive sources.
- The IPPAS team was informed that a dirty bomb exercise was conducted in Geneva. However, there are no regular exercises planned with license holders and emergency response organizations, such as the cantonal police, FOPH, SUVA, and NEOC. This will be considered in the second part of the RADISS Action Plan.

Basis: IAEA CoC, para 22 (o) states: “Every State should have in place an effective national legislative and regulatory system of control over the management and protection of radioactive sources. Such a system should: [...] have prepared, or has established provisions, to recover and restore appropriate control over orphan sources, and to deal with radiological emergencies and has established appropriate response plans and measures”

Recommendation 14: FOPH in collaboration with other competent authorities should establish a contingency plan to respond to malicious acts involving radioactive materials and ensure it is integrated with the national emergency plan.

Basis: NSS No.11-G, para 3.117. suggests: “Response measures should be developed based on information contained in the threat assessment and taking into consideration all foreseeable scenarios. These measures should be periodically exercised, reviewed and revised as necessary. The regulatory body should require the operator to implement appropriate response measures, for example by including the implementation of such response measures in the authorization conditions.”

Suggestion 16: FOPH and SUVA, in collaboration with other competent authorities, should consider periodically conducting training and security exercises and drills using appropriate scenarios that require the application of response procedures and guideline.

XIV.8 Detection and Reporting Nuclear Security Events

Art.127 and 129 of the RPO describes license holders' reporting requirements to the supervisory authority. The Guideline "Security of High Activity Radioactive Material" requires license holders to inform the cantonal police and implement response arrangements at a facility in the event of a security incident. These arrangements must be described in their security plan. Licensees are also required to conduct inventory verifications and report any loss or missing sources to competent authorities.

Unauthorized removal or sabotage of radioactive material must be reported to FOPH. FOPH reports this information to other competent authorities according to their guideline on intervention in the case of radiological incidents. License holders have to inform FOPH and SUVA (when applicable) of incidents no later than the following working day.

Art. 104 of the RPO includes a requirement for waste and recycling companies to detect and search for orphan radioactive materials (e.g., MORC). As part the RADISS Action Plan, FOPH published a guideline "Monitoring of wastes and recyclable materials for radioactivity" to facilitate the search and detection of MORC at these facilities. This document includes specific requirements and guidance for radiation detection measurements and includes clear instructions for reporting and securing radioactive materials.

The theme of detection is contained in the second field of action of the RADISS Action Plan. During the IPPAS mission, the FOPH provided information on the current status of the plan and described their efforts to enhance the detection of MORC at airports, borders and postal facilities. FOPH, in collaboration with the Federal Office of Customs and Border Security, Spiez Laboratory and PSI, has deployed temporary detection equipment at the main border crossing points to conduct random monitoring.

Figure 13: Radiation Portal Measures deployed at a border and handled by Customs



*Figure 14: temporary detection
deployed at a border and handled by Customs*

The IPPAS team was informed that FOPH has identified further deployment activities in phase 2 of the RADISS Action Plan. The IPPAS team encourages the State to continue its efforts to establish a permanent national detection strategy and implement permanent radiation detection measures at critical border points and strategic locations.

Basis: IAEA CoC, para 13 point b) states that “Every State should encourage bodies and persons likely to encounter orphan sources in the course of their operations, such as scrap metal recyclers and customs posts, to implement appropriate monitoring programmes to detect such sources.

Basis: NSS No.15, para 5.1. recommends: “The State should develop a national strategy for detection of a criminal act, or an unauthorized act, with nuclear security implications involving nuclear or other radioactive material that is out of regulatory control. The national detection strategy should be coordinated among and implemented by the competent authorities in accordance with assigned responsibilities, ideally with oversight by the coordination body.

Basis: NSS No.15, para 5.2. recommends: “Detection of nuclear and other radioactive material that is out of regulatory control can be achieved through an instrument alarm or an information alert. The State should design and implement nuclear security measures based on such indicators.”

Basis: NSS No.15, para 5.25. recommends: “The competent authority [...] should include budget and staff allocation necessary to operate and sustain the detection measures.”

Recommendation 15: The State and the competent authorities should establish and formalize its national strategy for detection of MORC. The competent authorities should implement and maintain permanent nuclear security measures at border crossings and other strategic locations to detect or provide an information alert for MORC and ensure that adequate human and financial resources are allocated for the training, operation and maintenance of these detection measures.

As part of its national threat assessment, the competent authorities should establish nuclear security measures for detecting MORC at locations where the likelihood of detection is maximized and at strategic locations. The IPPAS team provided a suggestion 7 on threat assessment under Chapter VI. IPPAS Mission is focused on the physical protection of nuclear materials and facilities, as well as radioactive material, associated facilities and associated activities. The IAEA also provides, upon

request, a service that is focused on MORC, therefore Switzerland could consider requesting the International Nuclear Security Advisory Service Mission (INSServ).

Overall, the IPPAS team found that Switzerland maintains cooperation and coordination to detect and report nuclear security events relating to radioactive materials.

XIV.9 Import and Export of Radioactive Sources

Switzerland has made a political commitment to the Code of Conduct (CoC) on the Safety and Security of Radioactive Sources, along with its two supplementary documents: “The Guidance on Import and Export of Radioactive Sources” and the Supplementary Guidance on the Management of Disused Radioactive Sources”. Switzerland has nominated FOPH as the point of contact for the purpose of sharing information and facilitating the export and import of radioactive sources.

The IPPAS team was informed that:

- The import and export of Category 1 and 2 sources is carried out in accordance with the CoC and its Guidance.
- In accordance with the RPO Annex 3 Activity level, every import of radioactive material must be authorized by the FOPH and requires a license.
- RPO Art. 103, requires a single import/export license for HASS.
- Consent and prior notification is required between countries and is implemented in Switzerland.
- Export of radioactive sources is only permitted when the sources are not considered as radioactive waste.
- FOPH encourages the return of radioactive sources to the supplier for reuse and recycling, when feasible.

Overall, the IPPAS Team found that FOPH follows the import and export provisions established in CoC and its supplementary guides.

XIV.10 Management of Disused Radioactive Sources

Switzerland adopted CoC and its supplementary guidance on the management of disused radioactive sources (DRS). FOPH encourages the return of DRS to the supplier state for reuse and recycling. In Switzerland, low activity DRS may be sent to PSI for long term storage and disposal. The IPPAS team was told that there is no strategy for the long-term management of disused HASS. In their license condition, PSI can only accept radioactive waste under 37 giga-becquerel (1 Curie) of activity for handling and conditioning as well as for intermediate storage, HASS is usually well above this limit. The IPPAS team noted that there is no policy for the long term safe and secure storage of DRS and no long-term storage facility for the permanent disposal of disused HASS.

Basis: IAEA CoC DRS Supplementary Guidance, para 11 states: “Each state should establish a national policy and strategy for the management of disused sources that reflects the State’s long term commitment to their safe and secure management.”

Basis: IAEA CoC DRS Supplementary Guidance, para 13 states: “Each State should ensure that State organizations with responsibilities for safety and security of radioactive sources, particularly the regulatory body, promote appropriate safety culture and security culture in their implementation of the

national policy and strategy and ensure the availability of appropriate programmes for the training of all those involved in the management of disused sources.”

Basis: IAEA DRS Supplementary Guidance, para 22 point (c) states: “Each State should ensure that a long-term storage facility is subject to a safety and security assessment prior to authorization by the regulatory body and is located, designed, constructed, operated, and decommissioned in conformance with regulatory requirements for safety and security”.

Recommendation 16: The State should consider establishing a policy and strategy for the long term management of disused HASS to ensure their safe and secure management. The State should consider establishing a long term storage facility for the safe and secure disposal of disused HASS.

XIV.11 Security of Radioactive Material in Transport

XIV.11.1 Transport security requirements and regulations

In Switzerland, transportation of Class 7 dangerous goods (radioactive materials) is subject to the ADR and the provisions in the RPA and RPO. The ADR provisions are integrated in the Ordinance on the transport of dangerous goods by road of 29 November 2002 (SDR). The IPPAS team was informed that radioactive sources in Switzerland are only transported by road. Some Category 2 (Security Level B) source arrive by air transport to Zurich airport which has a valid license approved by FOPH to temporarily store HASS in transit. SUVA inspected the safety and security measures at the airport to ensure they meet the security guideline for HASS.

FOPH, in collaboration with SUVA, is responsible for granting licenses for the transportation of radioactive materials that fall under their jurisdiction. The police in collaboration with SUVA or FOPH inspectors may conduct transport security verifications and they have been involved in the replacement of Category 1 or Category 2 sealed sources. The IPPAS team was informed that there is no formal security training for inspectors covering the protection of radioactive material during transport. The IPPAS team made a recommendation regarding training in XIV.1.2. FOPH has established transport security requirements in the HASS security guideline.

XIV.11.2 Security Management and Transport Security Plan

Transport security requirements for Category 1 to 3 radioactive sources are established in FOPH security guideline for HASS. As part of these requirements, the licensee is required to document its transport security measures in their general security plans. Additional information is requested for the transport of Security Level A in section 5.4. These security plans are reviewed and approved by FOPH in collaboration with SUVA for security level B. The table below describes the requirement for detection, delay and response.

In addition, SUVA published a best practice guide for security measures for the mobile use of high activity sealed sources in transport. This guide provides recommendations specific to non-destructive testing.

The prescriptive requirements described in the HASS guideline are based on ADR Chapter 1.10 and follow NSS No. 9-G.

FOPH HASS security guideline levels	IAEA NSS No. 9-G Levels
	Prudent management practice
Security level C	Basis security level
Security level A and B	Enhanced security level
	Additional security measures (for special circumstances)

Table 3: Transport security level established by FOPH

The IPPAS team was informed that there is no provision for additional security measures for increased threat level scenarios. In addition, there are no provisions to address low risk radioactive materials.

Basis: NSS No. 14, para 4.31. recommends that: “[...] the *graded approach* for transport security should be based at least on the properties and quantities of *radioactive material* being shipped:

- Material posing very low potential radiological consequences should be subject only to prudent management practices;
- Material with limited potential radiological consequences should be subject to basic security measures;
- Material posing higher potential radiological consequences should be subject to enhanced security measures.”

Basis: NSS No.14, para 4.34. recommends: “Enhanced security measures should include requiring that consignors, carriers, consignees and other persons engaged in the transport of *radioactive material* should develop, adopt, implement, periodically review as necessary and comply with the provisions of a transport security plan. Responsibility for and ownership of the transport security plan should be clearly defined. The plan should describe the overall *nuclear security system* in place to protect the *radioactive material* in transport and should include measures to address an increased *threat* level, response to *nuclear security events* and the protection of sensitive information.”

Basis: NSS No. 14, para 4.35. recommends: “In certain circumstances, security measures additional to those above should be considered depending on the assessment of the prevailing threat or the attractiveness of the material being transported. In such cases, possibly relevant only to certain categories or quantities of *radioactive material* or to particularly sensitive transports, additional security measures should be applied.”

Recommendation 17: FOPH should establish requirements to address increased threat levels during transport based on the recommended transport security measures in IAEA NSS 9-G (Rev.1), and should develop provisions for prudent management practices to follow a graded approach and enhance the security guidance regarding a transport security plan for Security Level A.

The IPPAS team observed that there is no specific requirement against sabotage. The IPPAS team made an observation on this issue in XIV.2.2.

XIV.11.3 **Implemented Detection, Delay and Response Measures**

These measures are described above.

XIV.11.4 **International Transport**

For international transport, the responsibility is on the licensee to ensure that security measures meet requirements. Import and export provisions apply and are described in XIV.9. In Switzerland, class 7 transport occur by road and the licensee must comply with the ADR and FOPH regulations. The IPPAS team was informed that Zurich airport has dedicated areas for the safe and secure temporary transit of class 7 radioactive materials to meet Ordinance on the Transport of Dangerous Good by Road (SDR) requirements and they are licensed and inspected by the supervisory authority.

COMPUTER SECURITY REVIEW (MODULE 5)

XVII. COMPUTER SECURITY STATE LEVEL REVIEW

XVII.1 Legal and Regulatory Framework

The last several years have seen a notable increase in highly visible cyber-attacks against nuclear facilities across many countries. Often these attacks have been for political or financial gain and haven't directly threatened the release of radiation, sabotage or theft of nuclear material. In that same time, we have seen very public occurrences of blended cyber physical attack on a massive scale in which it has been demonstrated that directed attacks against computer-based systems responsible for physical protection, nuclear safety and or nuclear material accountancy at nuclear facilities can have a serious impact on nuclear security, nuclear safety and nuclear operations. To address this threat, computer security must be a component of the state's regulatory framework and also of the facilities overall nuclear security programme.

In this period, Switzerland has taken several steps to advance the state of cyber security for critical sectors, many of which either directly or indirectly have the potential to significantly impact the state of cyber security readiness and response in nuclear facilities. For example, the creation of a Federal Office for Cyber Security (planned for 1 Jan of 2024) and the affiliation of the already existing National Cyber Security Centre is a natural evolution of the pre-existing Swiss nation state capability, and has the charter to provide a key role in the coordination of private and public organizations in the realm of computer security including critical infrastructure.

The ENSI is designated as the regulatory body for nuclear safety and security through authorities assigned in the following; Article 5 of the NEA – Preventive and protective measures, Article 9 of the NEO - Requirements concerning security, Article 10 of the NEO - Basic principles for the design of nuclear power plants, and Article 5(3) and Article 6(2) the DETEC TA&SM.

With respect to nuclear cyber security guidance, the relatively newly implemented *ENSI-G22 Cyber Security in Nuclear Installations – Guideline for Swiss Nuclear Installations*, provides a reference baseline to ensure the robust implementation of cyber security programs at all nuclear facilities. The legal basis for this guidance is spelled out in Section 2 as follows:

This guideline is based on Article 10 para. 2 and Article 12 para. 3 of the Nuclear Energy Ordinance of 10 December 2004 (NEO; SR 732.11) Article 5 par. 3 and Article 6 para. 2 of the DETEC Ordinance of 16 April 2008 on the Threat Assumptions and Security Measures for Nuclear Installations and Nuclear Materials (SR 732.112.1) and Article 70 para. 1 letter a of the Nuclear Energy Act of 21 March 2003 (NEA; SR 732.1).

In the five years since the IPPAS team conducted the initial Computer Security Review, ENSI and the nuclear facilities have made significant improvements to their respective nuclear cyber security capabilities and offerings. Most notable is the release of ENSI-G22 Computer Security in Nuclear Installations, Guideline for Swiss Nuclear Installations.

This document, and the included cyber threat assumptions (cyber DBT) leveraging nuclear security concepts from IAEA NSS and affiliated ISO 27000 series publications, provides a comprehensive high-

level basis for Swiss nuclear facilities to follow as they design, implement and operate digital systems throughout the country.

XVII.2 Roles and Responsibilities of the Competent Authority

Technical staff exchanges provide value to all involved, especially in a specialized area such as nuclear cyber security where an effective national capability is co-dependent upon a thorough understanding of; nuclear cyber centric threat information/collection, critical nuclear process and control systems as well as the potential consequences that can manifest when a coordinated blended cyber physical attack is directed at a particular facility.

In addition to the technical insight that such an exchange can provide, in the event of an actual incident response to an attack on significant systems (consider STUXNET - Natanz, Energetic Bear – Wolf Creek NPP and Kimsuky – Korea Hydro & Nuclear Power), existing relationships within the immediate response organizations can be vital to ensure effective and timely mitigation.

Basis: NSS No. 42-G, para 3.34. suggests: “The State should ensure that nuclear security systems and measures are in place at all competent authorities and operators in order to detect and assess computer security incidents that have actual or potential implications for nuclear security, and that relevant competent authorities are notified of such incidents so that appropriate response action can be implemented.”

Suggestion 17: ENSI should consider implementing staff exchanges between ENSI and the National Cyber Security Centre, potentially to include members of Cyber Battalion 42 and FIS staff in an attempt to familiarize each other with the skills, capabilities and personnel that exist as part of the larger Swiss nuclear cyber security capability.

Situations exist where industry specific targeted attacks can materialize in a very short period of time yet intelligence organizations can be hesitant to share knowledge of such things across even sensitive portals to a broad audience. Taking a proactive stance to formalize a chain of communication with pre-vetted individuals within critical facilities will ensure that emergency threat information can reach the appropriate plant officer as needed for immediate mitigation.

Basis: NSS No. 42-G, para 3.32. suggests: “The State should ensure that intelligence organizations provide appropriate support to contribute to or maintain an accurate and up to date national threat assessment that includes the threat of cyber-attacks against the nuclear security regime. Protocols and processes should be in place to support the transfer of information on cyberthreats to relevant entities within the nuclear security regime as appropriate to ensure adequate computer security against changing threats.”

Suggestion 18: ENSI should work with the appropriate officials (i.e., FIS, NCSC and the various stakeholders; NPPs, storage facilities, hospitals etc.) to ensure that there is a legal basis and formal implementation process to identify and deliver actionable threat intelligence in real time to responsible / vetted individuals at each nuclear facility.

The threat to nuclear facilities from cyber and blended cyber physical attack scenarios has expanded greatly in the last decade as multiple threat actors have turned their focus away from traditional computing targets to more strategic technical domains. Response to these advanced attack scenarios often requires the coordinated efforts of multiple organizations both within and potentially external to the nation that is under attack. It is in this area that the value of large-scale nuclear exercises becomes evident.

ENSI, the National Cyber Security Centre, NPP staff, Cyber Battalion 42 and others all stand to benefit from the investment of time and expertise that is required to generate and execute a national exercise in the Nuclear Cyber domain.

Basis: NSS No. 42-G, para 6.25. suggests: “The competent authority for computer security should ensure that nuclear security exercises are held with a computer security component to evaluate the State’s ability to response to computer security incidents, including blended attacks.”

Basis: NSS No. 42-G, para 6.26. suggests: “The Competent authority for computer security should ensure that competent authorities and operators conduct regular computer security exercises to train participants and validate their Computer Security Plans, including contingency plans. Where appropriate, these exercises should be integrated with other nuclear security exercises, and should periodically be conducted jointly with emergency exercises. Suggestion: Consider participating in a National or International multi-agency nuclear exercise with blended cyber and physical attack scenarios.”

Suggestion 19: ENSI should consider participating in a National or International multi-agency nuclear exercise with blended cyber and physical attack scenarios.

Much as there are physical inspections made prior to the loading of special materials for transport, cyber specific security actions and protocols must also be in play to ensure the integrity of the transport vehicle and the communications / tracking that takes place during the event.

ENSI has the technical ability to inform the approach taken by partner organizations regarding the real vulnerabilities and threat that exist in this space, and are very capable of providing advise on how to address these challenges. However, ENSI does not provide advice to the license holders.

Basis: NSS No. 33-T, para 4.87. suggests: “Technical control measures to limit access and ensure integrity should be applied to software and configuration files during development, transport, installation and operations.”

Basis: NSS No. 43-G IV–6 suggests: “Higher levels of capability are needed to ensure protection against highly capable threats or to prevent high radiological consequences. For example, competent authorities and operators that store, transport, or use Category I or II nuclear material, or operate facilities or perform activities that have the potential for high radiological consequences, are considered to be managing very high or high consequences.”

Suggestion 20: ENSI should consider advising partner authorities relying on its ability to make technical recommendations regarding the validation of the security status of transport vehicles, and based on a graded approach as it relates to digital systems involved in the secure operation and material tracking during transport.

Commodity digital processing components - often down to the chip level on large batch sub-systems, have the potential to contain capabilities that at a cursory level are not visible to a downstream systems integrator and especially if not intentionally “enabled” can lie dormant throughout the inspection process only to manifest post deployment.

There are also a variety of engineering reasons whereby an otherwise stalwart employee or sub-contractor may seek to deploy a “temporary” connection to facilitate an upgrade or similar process.

Basis: NSS No. 42-G, para 3.20. suggests: "Computer security plays an important role in the interface between nuclear security and nuclear safety, especially in view of the increasing reliance on computer based systems within all operational aspects of nuclear facilities."

Suggestion 21:

While guideline ENSI-G22 Cyber Security in Nuclear Installations defines clear high-level requirements for all processes related to the use of sensitive computer systems to consider the whole lifecycle of the respective systems, the IPPAS noted that from the safety perspective neither guideline ENSI-A04 Documentation of permit-relevant modifications in nuclear power plants nor guideline ENSI-B14 Maintenance of safety classified equipment electrical and I&C equipment has a clearly defined interface with cyber security regarding the systems lifecycle. Yet, both NSS 33-T section 4 as well as NSS 42-G, Annex I, paragraph 22, suggests to implemented measures to protect sensitive digital assets from compromise throughout their life cycle in accordance with the concepts of a graded approach and defence in depth.

This lack of specificity may lead to ambiguity in the practical implementation of Safety and or Security measures across the impacted platforms. There is value in working proactively with all parties involved to establish an agreed upon approach (consider a flow diagram or similar) in which a determination on how to proceed that considers risk, compliance, safety and operational impact can be successfully resolved in a timely manner.

Basis: NSS No. 42-G, para 7.15. suggests: "If the results of the risk assessment deviate significantly from what has been assumed by the competent authority for computer security, then the competent authorities or operators should resolve this issue in a timely manner. Such deviations might result from, for example, changes in the local threat environment or equipment changes introducing new vulnerabilities."

Suggestion 22: The ENSI should consider evaluating how the interface between I&C-related safety requirements (e.g., ENSI-A04 and ENSI-B14) and ENSI-G22 could be improved to facilitate the applying of a graded approach when assessing IT-related changes at I&C systems.

Computer security programs evolve over time and often go through classic stages. This process tends to be driven by multiple factors, often involving a gradual awareness of additional threats as internal capabilities expand within both the regulatory authority and the onsite cyber staff. To ensure both programmatic efficacy and the identification of potential areas for future development, a comprehensive self-assessment is recommended with annual updates focused on specific cyber sub-domains.

IAEA's NST-037 (TDL006) Conducting Computer Security Assessments provides an excellent overview of this process while, National Institute of Technology (NIST), International Electrotechnical Commission (IEC) and US Department of Energy all provide excellent guidance as well. For consideration, it is worth pointing out that although derived in the United States, the Cyber Security Maturity Model, C2M2 was co-developed with US private energy corporations and contains nuclear security specific content. There is also an automated program that can be utilized to step through the assessment, provide status reporting in each cyber domain and then track performance trending over time. To date, several non-US countries have implemented this capability in their environments.

Basis: IAEA NST-037, para 1.1. suggests: "A rigorous, comprehensive assessment process can assist in strengthening the effectiveness of a facility's (and State's) computer security programme."

Suggestion 23: With the publication of ENSI-G22 and recent digital upgrades that have taken place across the Swiss nuclear regime, this would be a good time to execute a detailed baseline analysis at the facility level through the performance of a comprehensive self-assessment.

Good Practice 10: The demonstrably high level of technical competency within the ENSI nuclear cyber team allows for performance-based engagement and oversight that is not typically found in regulatory agencies. Coupled with the exhaustive implementation of cyber integration into facility permitting processes, ENSI staff are able to establish and maintain a very detailed understanding of digital systems deployment and status regarding current cyber security posture at each facility.

Note: there is a potential “downside” to this approach as great care must be taken to ensure the long-term viability of the team. Nuclear cyber security is a highly competitive field and individuals with deep technical knowledge are sought after in many related critical infrastructure sectors. ENSI will need to remain vigilant to ensure that staff positions are competitive and rewarding as a long-term career option with a focus on identifying, attracting and retaining similarly competent resources in the future.

XVIII. COMPUTER SECURITY FACILITY LEVEL REVIEW

ACKNOWLEDGEMENTS

The IPPAS team received an outstanding cooperation from all personnel at all levels. Competent authorities and other stakeholders provided valuable information in a transparent manner for the team. Practical arrangements made by ENSI, SFOE, FOPH, DETEC, Cantonal police of Aargau, operators of Leibstadt NPP, Beznau NPP, ZWILAG Central Interim Storage Facility, CHUV and LorNDT were excellent.

The IPPAS team would like to recognize the outstanding work done in the Advance Information Package.

All personnel at all levels were willing to share their knowledge and experience with the team. Informal discussions between the team and persons from the host country participating the mission provided the platform for both parties to learn more about nuclear security.

Commitment by the high management of ENSI, SFOE, FOPH and DETEC was present during the meetings and discussions.

In addition, the team acknowledges the hospitality of host country representatives welcoming the experts. Flexibility to achieve the objectives of the mission was excellent and highly appreciated. Experts of ENSI also took an initiative in a short time to provide the IAEA Office of Public Information and Communication experts an opportunity to prepare the International Conference on Nuclear Security 2024 during the busy IPPAS follow-up mission.

APPENDIX I: SYNOPSIS OF RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES

Module 1

Recommendation 1: ENSI should define NMAC objectives and provisions for nuclear security purposes to the attention of the licensees following a graded approach that would consider also the physical and chemical form of the nuclear material and the associated insider risks, in particular the risks associated to the protracted theft.

Recommendation 2: The State should further clarify the conditions under which modifications affecting nuclear security require a permit or an amendment to the license.

Recommendation 3: The competent authorities should formalize arrangements for the communication and exchange of information between relevant stakeholders with nuclear security responsibilities in order to achieve regular, comprehensible and formalized interaction.

Recommendation 4: The State should conduct an assessment of its categorization process against the A/CPPNM to ensure that a graded approach is applied in protection of all nuclear material, in any quantity, that could be used in a nuclear explosive device. Based on the assessment, the State should take appropriate actions.

Recommendation 5: The State should develop and establish a graded approach for protection of nuclear material and systems, structures and components against sabotage based on radiological consequences.

Suggestion 1: The State should consider formalizing the management of the interfaces between safety and security in order to systematically identify potential conflicts and to ensure that nuclear security measures do not compromise nuclear safety and safety measures do not compromise nuclear security.

Suggestion 2: The State should consider formalizing cooperation between ENSI and SFOE in order to improve the efficiency of the use of NMAC for nuclear security purposes.

Suggestion 3: The State should consider continue ensuring that the terms “safety” and “security” are consistently distinguished in legal documents.

Suggestion 4: The State should consider continuing to address cybersecurity in the legally binding documents on statutory and secondary legislation level in order to clearly define responsibilities of all involved entities for correctly interpreting and implementing their legal obligations related to computer security.

Suggestion 5: Following Recommendation 2 above, ENSI should consider defining clearly the security classification and identify what SSC and equipment subject to this classification.

Suggestion 6: ENSI should consider developing and implementing basic security training program for site inspectors in order to include basic security considerations during their weekly on-site inspections.

Suggestion 7: The State should consider providing written documentation of the national threat assessment for the competent authorities in order to develop a Design Basis Threat.

Suggestion 8: ENSI and FOCS/NCSC should consider formalizing their mutual information exchange by implementing a MoU.

Suggestion 9: ENSI should consider evaluating evolving threats posed to Swiss nuclear installations by uncrewed vehicles.

Suggestion 10: As a basis for the graded approach for protection against unauthorized removal and sabotage of Low Level Wastes and Intermediate Level Wastes which are not nuclear material, the State should consider defining clear links between categories of these radioactive wastes and the different security zones mentioned in Annex 2 of the NEO. The categorization of these wastes could be based on NSS No. 11-G.

Suggestion 11: ENSI should consider establishing requirements regarding the plant specific assessments of potential insider threats for security personal, especially for personnel in highly sensitive positions like the CAS.

Suggestion 12: ENSI should consider conducting an analysis that would take into account risks associated to insiders using explosives in order to determine what could be the appropriate frequency of searches for explosives for both persons and vehicles.

Suggestion 13: ENSI should consider that when addressing the nuclear security culture topic, specific emphasis should be placed on confidentiality, trustworthiness, the belief that a threat exists and that the associated radiological consequences could be high.

Suggestion 14: The State should consider developing a coherent and consistent national policy regarding the security of nuclear sensitive information, in particular regarding the classification ranks and rules, across all facilities, sites and organizations (governmental and non-governmental) handling nuclear sensitive information.

Good Practice 1: ENSI regularly and actively participates in international events in the field of nuclear security and regularly invites international peer review missions for which it has undertaken as a commitment in legally binding documents in order to continuously improve nuclear safety and security and to strengthen nuclear supervision through active participation in the international regulatory exchange of information and experience.

Good Practice 2: The rights and duties of the operator`s security guards in the case of nuclear security events are based on a precise, comprehensive and binding legal basis.

Module 2

Suggestion 15:

Suggestion 16:

Module 4

Recommendation 6: FOPH and SUVA should develop and implement a formalized training programme for inspectors on the security of radioactive materials as part of their learning management system to maintain the competence and to strengthen capacity building of personnel assigned to security functions.

Recommendation 7: FOPH and SUVA should continue promoting and implementing an over-arching nuclear security policy that recognizes that credible threats exist, and that preserving nuclear security of radioactive material is important. In addition, the competent authorities should consider promoting and supporting nuclear security culture for radioactive materials.

Recommendation 8: The State should establish a long term plan to maintain the effective communication, collaboration and cooperation among competent authorities established under the RADISS Action plan and to ensure that sufficient resources are committed for secure use of radioactive materials at the national level and to sustain its nuclear security regime.

Recommendation 9: The State should explicitly mention security of radioactive material at the appropriate regulatory level to provide clarity and consistency and establish requirements for the security of radioactive sources in alignment with the appropriate security guideline and ordinances.

Recommendation 10: The State should ensure that FOPH personnel with security responsibilities for radioactive material with access to sensitive information or HASS undergo a trustworthiness verification that include a criminal background checks.

Recommendation 11: The competent authorities should establish bilateral and multilateral agreements in case of loss of control of radioactive sources or any security incidents with potential transboundary effects.

Recommendation 12: The State should assess and periodically review the national threat and describe the motivations, intentions and capabilities of potential adversaries, including the threat of insiders to commit malicious acts to radioactive materials, associated facilities and associated activities and to inform relevant competent authorities. FOPH should use the results of the threat assessment as a common basis for determining security requirements for designing and evaluating of the security systems for radioactive materials, associated facilities and associated activities.

Recommendation 13: The State should ensure that FOPH has sufficient human and financial resources to develop and sustain competence, capacity and compliance activities to ensure the oversight of safety and security of radioactive materials.

Recommendation 14: FOPH in collaboration with other competent authorities should establish a contingency plan to respond to malicious acts involving radioactive materials and ensure it is integrated with the national emergency plan.

Recommendation 15: The State and the competent authorities should establish and formalize its national strategy for detection of MORC. The competent authorities should implement and maintain permanent nuclear security measures at border crossings and other strategic locations to detect or provide an information alert for MORC and ensure that adequate human and financial resources are allocated for the training, operation and maintenance of these detection measures.

Recommendation 16: The State should consider establishing a policy and strategy for the long term management of disused HASS to ensure their safe and secure management. The State should consider establishing a long term storage facility for the safe and secure disposal of disused HASS.

Recommendation 17: FOPH should establish requirements to address increased threat levels during transport based on the recommended transport security measures in IAEA NSS 9-G (Rev.1), and should develop provisions for prudent management practices to follow a graded approach and enhance the security guidance regarding a transport security plan for Security Level A.

Recommendation 18:

Suggestion 17: FOPH, in collaboration with relevant competent authorities should consider revising the HASS security guideline to fully align with international guidance established in IAEA NSS 11-G (Rev-1), NSS 43-G and NSS 23-G.

Suggestion 18: FOPH and SUVA, in collaboration with other competent authorities, should consider periodically conducting training and security exercises and drills using appropriate scenarios that require the application of response procedures and guideline.

Suggestion 19:

Suggestion 20:

Suggestion 21:

Suggestion 22:

Suggestion 23:

Suggestion 24:

Suggestion 25:

Suggestion 26:

Suggestion 27:

Suggestion 28:

Suggestion 29:

Suggestion 30:

Suggestion 31:**Suggestion 32:**

Good Practice 3: The IPPAS team commends the efforts lead by FOPH and compliment the outstanding collaboration and cooperation of the federal organizations that contributed to the success and accomplishment of the RADISS Action Plan. The active collaboration, coordination and cooperation among competent authorities will significantly enhance the safety and security of radioactive materials in Switzerland.

Good Practice 4: A national action plan has been established to enhance the safety and security of radioactive materials and involves representatives from the regulatory bodies, law enforcement, national security, criminal prosecution and intelligence community and other relevant organizations. The Action Plan contains a solid legal basis, strategy and three thematic areas with clear priorities and measurable objectives and timelines.

Good Practice 5: FOPH requires licensees to justify the use of ionizing source in terms of associated benefits and risk to society and have developed a comprehensive guideline for HASS justification. This document contains instructions on how to assess the application and includes security risk factors and a review of available alternative technologies. The objective is to phase out HASS when equivalent alternative technologies can be used, therefore permanently eliminating the risk related to HASS.

Good Practice 6: The regulator requires HASS license holders to conduct regular self-assessment of their security measures and provide guidance and a detailed list of items to verify to meet this objective. This self-assessment may be reviewed by the regulator upon request.

Good Practice 7: The regulator provides detailed intrusion detection system requirements and requires the certification of security system installers. These criteria are based on established industry security standards. Certified barriers must also be installed and meet certain resistance criteria. The barrier resistance classes include the intruder profile, tools required and break-in time. These requirements are very clear for the regulator and licensees which makes them easy to review and accept during the licensing and supervision activities.

Good Practice 8: FOPH has established a modern, online national e-registry for Category 1 to 5 sealed sources, unsealed sources and other ionizing radiation devices that is shared with other competent authorities, including the canton police forces, and security intelligence services to share relevant information and to coordinate security efforts.

Good Practice 9: FOPH and their collaborators have prioritized the replacement of blood irradiators with alternative technologies, therefore permanently reducing the associated risk of malicious acts.

Good Practice 10:**Good Practice 11:****Good Practice 12:**

Good Practice 13: CHUV replaced Category 2 source (Security Level B) with alternative technologies therefore minimizing the potential radiological risk.

Good Practice 14:

Good Practice 15:

Good Practice 16:

Module 5

Suggestion 33: ENSI should consider implementing staff exchanges between ENSI and the National Cyber Security Centre, potentially to include members of Cyber Battalion 42 and FIS staff in an attempt to familiarize each other with the skills, capabilities and personnel that exist as part of the larger Swiss nuclear cyber security capability.

Suggestion 34: ENSI should work with the appropriate officials (i.e., FIS, NCSC and the various stakeholders; NPPs, storage facilities, hospitals etc.) to ensure that there is a legal basis and formal implementation process to identify and deliver actionable threat intelligence in real time to responsible / vetted individuals at each nuclear facility.

Suggestion 35: ENSI should consider participating in a National or International multi-agency nuclear exercise with blended cyber and physical attack scenarios.

Suggestion 36: ENSI should consider advising partner authorities relying on its ability to make technical recommendations regarding the validation of the security status of transport vehicles, and based on a graded approach as it relates to digital systems involved in the secure operation and material tracking during transport.

Suggestion 37:

Suggestion 38: The ENSI should consider evaluating how the interface between I&C-related safety requirements (e.g., ENSI-A04 and ENSI-B14) and ENSI-G22 could be improved to facilitate the applying of a graded approach when assessing IT-related changes at I&C systems.

Suggestion 39: With the publication of ENSI-G22 and recent digital upgrades that have taken place across the Swiss nuclear regime, this would be a good time to execute a detailed baseline analysis at the facility level through the performance of a comprehensive self-assessment.

Good Practice 17: The demonstrably high level of technical competency within the ENSI nuclear cyber team allows for performance-based engagement and oversight that is not typically found in regulatory agencies. Coupled with the exhaustive implementation of cyber integration into facility permitting processes, ENSI staff are able to establish and maintain a very detailed understanding of digital systems deployment and status regarding current cyber security posture at each facility.

APPENDIX II: IPPAS TEAM COMPOSITION

██████████ (IPPAS Team Leader), Nuclear Safety Council (CSN), Spain

██████████, Federal Agency for Nuclear Control (FANC), Belgium

██████████, Canadian Nuclear Safety Commission (CNSC), Canada

██████████, State Office for Nuclear Safety (SONS), Czech Republic

██████████, Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV), Germany

██████████, Istanbul Technical University (ITU), Türkiye

██████████, Office for Nuclear Regulation (ONR), United Kingdom

██████████, Sandia National Laboratories (SNL), United States of America

Technical Officer

██████████, IAEA

APPENDIX III: HOST COUNTRY COUNTERPARTS

Swiss Federal Nuclear Safety Inspectorate ENSI

Director General

Director, Division of Radiation Protection

Chief of Staff

Head, Section of Nuclear & Cyber Security, Deputy Liaison Officer with the IAEA

Deputy Head, Section of Nuclear & Cyber Security

Nuclear & Cyber Security Specialist

Nuclear & Cyber Security Specialist

Nuclear Security Specialist

Nuclear Security Specialist

Head of International Affairs, Liaison Officer with the IAEA

Head of Legal Affairs

Attorney at Law, Specialist Legal Affairs

Head, Occupational Radiation Protection Section

Deputy Head, Section of Transports and Predisposal

Specialist, Human and Organisational Factors

Swiss Federal Office of Energy

Deputy Director SFOE, Division of Supervision and Safety

Specialist, International Nuclear Energy Affairs, Liaison Officer for the SFOE

Head, Safeguards Section

Safeguards Specialist

Specialist, Nuclear Energy Law

IT-Security Specialist

Federal Office of Public Health

Deputy Director FOPH, Head Health Protection Directorate

Head, Division of Radiation Protection

Head, Section of Research Facilities and Nuclear Medicine

Project Manager Action Plan Radiss, Liaison Officer for the FOPH

Radiation Protection Specialist

Federal Department of the Environment, Transport, Energy and Communications (DETEC)

Secretary General

Advisor

National Cyber Security Centre

Deputy Head Operational Cybersecurity OCS

Swiss Federal Accident Insurance Fund SUVA

Radiation Protection Specialist

Federal Intelligence Service FIS

Federal Intelligence Specialist

Swiss Federal Police fedpol

Deputy Head, International Police Cooperation, Head of Division Operations Center/SIRENE Switzerland

Cantonal Police of Aargau

Captain, Head of the Leadership and Deployment

Canton Aargau

Cantonal Command Staff

Nuclear Power Plant Beznau

Head of plant security at NPP Beznau

Nuclear Power Plant Gösgen

Chief Information Security Officer

ICT Security Engineer

Nuclear Power Plant Leibstadt

Deputy Head Security

Deputy Head Guard Group

Chief Information Security Officer

Information Security Officer

Computer Security Engineer

Central Interim Storage Facility ZWILAG

Chief Security Officer, Fire Protection Engineer

Swiss University Hospital Lausanne CHUV

Head of Security

Deputy Head Security

Team Security

Head Medical Physics Radiooncology

Radiation Protection IRA

Radiation Protection IRA

Medical Physics Radiooncology

Lor NDT

Co-Founder and Holder