

NOTE: This version is a sanitized version and restricted/confidential (Act on the Openness of Government Activities 621/1999, Section 24 (1) (7) **parts of the Mission Report have been deleted and marked in the document by the Finnish Radiation and Nuclear Safety Authority (STUK). This sanitized version is categorized as Public.**

INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)



INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

IPPAS Mission Report:

Finland

6-17 June 2022

Prepared for the Ministry of Economic Affairs and Employment

[REDACTED]

Distribution of this IPPAS mission report, designated as 'Highly Confidential', is at the discretion of the Government of the Finland¹. The IAEA will make the report available to third parties only with the express permission of the Government of the Finland. 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.

[REDACTED]

ABBREVIATIONS

ADR	Agreement concerning the International Carriage of Dangerous Goods by Road
CAS	Central Alarm Station
CBRNE	Chemical Biological Radiological Nuclear Explosive
CCTV	Closed Circuit Television
CoC	Code of Conduct on the Safety and Security of Radioactive Sources
CPPNM/A	Amended Convention on Physical Protection of Nuclear Material
CSIRT	Cyber Security Incident Response Team
DBT	Design Basis Threat
EPR	European Pressured Reactor
HASS	High Activity Sealed Source
HRC	High Radiological Consequence
HVM	Hostile Vehicle Mitigation
IAEA	International Atomic Energy Agency
IPPAS	International Physical Protection Advisory Service
ITDB	Incident and Trafficking Database
I&C	Instrumentation and Control
MCR	Main Control Room
MEAE	Ministry of Economic Affairs and Employment
MSAH	Ministry of Social Affairs and Health
NCSC-FI	National Cyber Security Center
NDT	Non Destructive Testing
NEA	Nuclear Energy Act
NED	Nuclear Energy Decree
NIST	National Institute of Standards and Technology (US)
NMAC	Nuclear Material Accounting and Control
NPP	Nuclear Power Plant
NSO	Nuclear Security Officer
NSS	IAEA Nuclear Security Series
OL3	Olkiluoto 3
PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
RPM	Radiation Portal Monitor
RSO	Radiation Safety Officer



SDA	Sensitive Data Asset
SSCs	Structures, Systems, Components
STO	STUK Department of Radiation Practices Regulation
STUK	Finnish Radiation and Nuclear Safety Authority
SUPO	Finnish security and Intelligence Service
TAV	STUK Department of Radiation in Industry and Occupational Exposure Section
TRAFICOM	Finnish Transport and Communications Agency
TVO	Teollisuuden Voima Oyj
Tykslab	Turku University Hospital laboratory
URC	Unacceptable Radiological Consequence
VIRT	Virtual Incident Response Team
WANO	World Association of Nuclear Operators
YTO	STUK Department of Nuclear Reactor Regulation
YTS	STUK Section for Nuclear Security



CONTENTS

ABBREVIATIONS	3
CONTENTS	5
SUMMARY.....	9
I. INTRODUCTION.....	12
I.1 Objectives.....	12
I.2 Scope	13
NATIONAL REVIEW OF NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL (MODULE 1)	14
II. GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION.....	14
II.1 Legislative Branch.....	14
II.2 Executive Branch	15
II.3 Judicial Branch.....	17
II.4 Safety, Security and Safeguards in Finland	18
III. LEGISLATIVE AND REGULATORY FRAMEWORK	19
III.1.1 International Instruments	19
III.1.2 Laws and Secondary Legislation	23
III.1.3 Regulations and Technical Guidance.....	26
IV. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY	28
IV.1 Cooperation within STUK	29
IV.2 Licensing/Authorization Process.....	30
IV.2.1 The Decision-in-Principle	30
IV.2.2 The Construction License	31
IV.2.3 The Construction.....	32
IV.2.4 The Operational License and the Commissioning phase	32
IV.3 Inspection and Enforcement.....	32
IV.4 Coordination with Other State Organizations that Contribute to Nuclear Security	34
IV.4.1 Advisory Commission on Nuclear Security.....	34
IV.4.2 Practical arrangements with local authorities	35

V.	THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)	36
VI.	RISK INFORMED APPROACH	38
VI.1	Risk Management	39
VI.2	Graded Approach	39
VI.2.1	Risk of unauthorized removal of nuclear material	40
VI.2.2	Risk of sabotage	41
VI.3	Defence in Depth	42
VII.	SUSTAINING THE PHYSICAL PROTECTION REGIME	43
VII.1	Security Culture	43
VII.2	Quality Assurance	44
VII.3	Confidentiality and Trustworthiness	45
VII.3.1	Confidentiality	45
VII.3.2	Trustworthiness	46
VII.4	Sustainability Programme	47
VIII.	PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS	48
VIII.1	Contingency Planning at the National Level	48
VIII.2	Emergency and Contingency Planning Interface	48
	NUCLEAR FACILITY REVIEW (MODULE 2)	49
IX.	OLKILUOTO 3 NUCLEAR POWER PLANT (NPP)	49
IX.1	Security Management Programme	50
IX.1.1	Threat and Target Identification	50
IX.1.2	Security Plan including Contingency Plan	52
IX.1.3	Interfaces with Nuclear Safety and Nuclear Material Accounting and Control	52
IX.1.4	Security Organization	52
IX.1.5	Security Staff Training and Qualification	53
IX.1.6	Security Culture	54
IX.1.7	Security Procedures	55
IX.1.8	Confidentiality and Trustworthiness	55
IX.1.9	Reporting of Nuclear Security Events	55
IX.1.10	System Evaluation, including Performance	56
IX.1.11	Quality Assurance	56
IX.1.12	Sustainability Programme	57
IX.2	Physical Protection System (PPS)	57

IX.2.1	Graded Protection and Defence in Depth	57
IX.2.2	Detection	58
IX.2.3	Access Control	61
IX.2.4	Central Alarm Station	62
IX.2.5	Delay	64
IX.2.6	Response	65

SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4)..... 66

X. NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL..... 66

X.1	Assignment of Nuclear Security Responsibilities	66
X.1.1	State.....	66
X.1.2	Regulatory body	66
X.1.3	Other Competent Authorities	69
X.1.4	Operator, Shipper and/or Carrier	69
X.2	Legislative and Regulatory Framework	70
X.2.1	Laws	70
X.2.2	Regulations.....	72
X.2.3	Trustworthiness verification	74
X.2.4	National Registry and Inventory of Radioactive Sources.....	75
X.3	International Cooperation and Assistance.....	76
X.4	Identification and Assessment of Threats	76
X.5	Risk Based Nuclear Security Systems and Measures	77
X.5.1	Risk Management	77
X.5.2	Interface with the Safety System	77
X.6	Sustaining the Nuclear Security Regime.....	78
X.7	Planning and Preparedness for and Response to Nuclear Security Events	80
X.8	Detection and Reporting of Nuclear Security Events	81
X.9	Import and Export of Radioactive Sources	82
X.10	Security of Radioactive Material in Transport.....	82
X.10.1	Transport Security Requirements and Regulations.....	82
X.10.2	Security Management and Transport Security Plan.....	84
X.10.3	Implemented Detection, Delay and Response Measures	85
X.10.4	International Transport.....	86

XI. FACILITY LEVEL REVIEW 87

XI.1	Turku University Hospital Laboratory (Tykslab)	87
XI.1.1	Security Management	89
XI.1.2	Security System	91
XI.2	Olkiluoto NPP	95
XI.2.1	Security Management	96
XI.2.2	Security System	96
COMPUTER SECURITY REVIEW (MODULE 5).....		100
XII.	COMPUTER SECURITY STATE LEVEL REVIEW.....	100
XII.1	Legal and regulatory framework	100
XII.2	Roles and responsibilities of competent authorities	102
XIII.	COMPUTER SECURITY FACILITY LEVEL REVIEW	103
XIII.1	Computer Security at Olkiluoto NPP	103
XIII.1.1	Computer Security Policy	104
XIII.1.2	Asset Management	104
XIII.1.3	Physical Protection and Environmental Security	105
XIII.1.4	Computer Operations Management	105
XIII.1.5	Computer Access Control	106
XIII.1.6	Computer Acquisition, Development and Maintenance	106
XIII.1.7	Incident Management	106
XIII.1.8	Continuity Management	107
ACKNOWLEDGEMENTS.....		109
APPENDIX I: SYNOPSIS OF RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES.....		110
APPENDIX II: IPPAS TEAM COMPOSITION.....		116
APPENDIX III: HOST COUNTRY COUNTERPARTS.....		117

SUMMARY

(Public) This report presents the results of the International Atomic Energy Agency (IAEA) International Physical Protection Advisory Service (IPPAS) mission conducted in Finland from 6 to 17 June 2022. This is the 97th IPPAS mission of IAEA and the third mission hosted by Finland. Previous missions were held in 2009 and 2012.

(Public) Prior to the mission, a preparatory meeting was conducted in January 2020, during which arrangements for the mission were discussed and agreed upon.

(Public) The objectives of the IPPAS mission were the following: to review current status of the national nuclear security regime for nuclear and other radioactive material and associated facilities and activities, including transport of radioactive material; review the implementation of nuclear security measures at Olkiluoto Nuclear Power Plant operated by TVO and nuclear security practice of high activity radioactive sources at Turku University Hospital Laboratory (Tykslab); compare the procedures and practices of Finland with the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment (A/CPPNM); Code of Conduct on Safety and Security of Radioactive Sources, Nuclear Security Series (NSS) No. 20, Objectives and Essential Elements of a States Nuclear Security Regime; IAEA NSS No. 13 / INFCIRC/225/Rev.5, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities; IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities and with other relevant IAEA NSS documents; provide advice for continued improvement of nuclear security; and identify good practices.

(Public) The scope of the mission covered four IPPAS modules, including National Review of Nuclear Security Regime for Nuclear Material and Nuclear Facilities (Module 1), Nuclear Facility Review (Module 2), Security of Radioactive Material, Associated Facilities and Associated Activities (Module 4), and Computer Security Review (Module 5). The issues related to nuclear security interfaces with nuclear material accountancy and control, and safety were also addressed during the mission. The IPPAS mission did not include a review of the Security during Transport of Nuclear Material (Module 3).

(Public) For this IPPAS mission, the IAEA assembled a ten person team comprised of experts from nine nations and the IAEA. The IPPAS mission team members were from: Switzerland; Belgium; Canada; Czech Republic; France; Hungary; Japan; United Kingdom; United States of America and IAEA. The experts have broad expertise and extensive experience in nuclear legislation, regulatory oversight, physical protection system design, implementation and assessment, including computer security. During the mission, the IPPAS team interacted with key personnel from the Finnish Radiation and Nuclear Safety Authority (STUK), Ministry of Defence, Ministry of Economic Affairs and Employment, Ministry of the Interior, Finnish Customs, Finnish Border Guard, National Police Board, Southwestern Finland Police Department and Finnish Security and Intelligence Service, as well as management and staff from the facilities visited.

(Public) It was apparent to the IPPAS team that significant time and effort was invested by STUK and other participants in the preparation and conduct of the mission. STUK provided the IAEA and the IPPAS team members with a comprehensive Advance Information Package consisting of relevant information related to Finland's legislative and regulatory framework, roles and responsibilities of the

[REDACTED]

competent authorities and other Finnish organizations involved in nuclear security, as well as information on nuclear facilities and activities. The relevant Finnish legal and regulatory documents on nuclear security were also included in the Advance Information Package. The IPPAS team would like to acknowledge Finland's efforts in supporting an IPPAS mission during the time of a pandemic (COVID-19). These efforts of the host country demonstrate a strong commitment to nuclear security.

(Public) The IPPAS team observed that the nuclear security regime in Finland is well established, and incorporates the fundamental principles of the CPPNM and its Amendment. It is also aligned with the IAEA nuclear security guidance. The team provided advice, in the form of recommendations and suggestions, to support Finland in enhancing and sustaining nuclear security; good practices were identified that can serve as examples to other IAEA Member States to help strengthen their nuclear security regimes. Finland is adhering and contributing to all international instruments relevant to nuclear security and its nuclear security legislation is continually being reviewed and updated as necessary.

(Public) The IPPAS team identified a number of good practices. Finland benefits from a mature, balanced and coordinated inter-ministerial partnership to support the nuclear security regime. The internal cooperation between STUK's entities in supporting nuclear security activities is also well established. The regular review of the legal and regulatory framework relating to nuclear security combined with the Design Basis Threats helps to ensure that the current evaluation of the threat is reflected in legal requirements. Availability of well-coordinated on-site and off-site response forces provide a strong and flexible means to respond to a large range of nuclear security events at nuclear facilities. The IPPAS team recognizes the establishment of an effective joint command and control structure to respond to nuclear security events.

The IPPAS team acknowledges that there are areas which should be addressed in order to sustain the current level of regulatory assurance for nuclear security. Staffing capacity for nuclear security should be considered, and promoting nuclear security in the integrated culture towards a more balanced status at STUK should be addressed. Integrating competencies and capabilities of the various stakeholders in the field of computer security needs improvement. [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

(Public) The IPPAS team realizes that the challenges inherent in successfully completing the cyber security migration from construction phase to full operations is a highly complex effort. Olkiluoto 3 is quickly approaching a nexus of increased complexity (final takeover and control of the multiple critical I&C environments from the contractor) and evolving threat. A major focus of enhanced cyber resources and leveraged "lessons learned" from the international community may be beneficial.

(Public) Since the previous IPPAS mission STUK has made significant progress in enhancing the security of radioactive materials in Finland. The IPPAS team noted areas for improvements in the implementation of security culture, information protection, trustworthiness and enforcement of security requirements for radioactive materials. The regulatory framework for the security of radioactive materials needs to be revised to better align with IAEA recommendations and guidance. Efforts are needed to allocate additional resources and to build appropriate competence for security inspections of radioactive material in use, storage and transport to ensure oversight functions of STUK. Further efforts should be made to enhance collaboration between the operators and the local police.

(Public) The IPPAS team commends STUK for their well-established interface between safety and security to ensure the security of radioactive materials.

[REDACTED]

[REDACTED]

| (Public) A total of 19 Recommendations and 31 Suggestions were provided which could enhance nuclear security. In addition, a total of 11 Good Practices were identified during the mission, which, if shared, could benefit other Member States in enhancing nuclear security.

| (Public) In conclusion, the IPPAS team assesses that Finland has a mature and well-established nuclear security regime, which has been continually enhanced in recent years.

| (Public) The mission report is treated by the IAEA as “Highly Confidential” and protected accordingly. Distribution of this IPPAS mission report is at the discretion of the Government of Finland. The IAEA will make the report available to third parties only with the express permission of the Government of Finland.

[REDACTED]

I. INTRODUCTION

(Public) Since its inception in 1995, the purpose of the International Atomic Energy Agency's (IAEA) International Physical Protection Advisory Service (IPPAS) has been to provide advice and assistance to strengthen the effectiveness of a State's physical protection regime for nuclear material and nuclear facilities.

(Public) This report presents the results of the IAEA's IPPAS mission conducted in Finland from 6 to 17 June 2022. This was the IAEA's 97th IPPAS mission, and the third IPPAS mission in Finland. The first IPPAS mission in Finland was conducted in 2009 and the second in 2012.

(Public) This mission was requested by Finland in March 2019 (letter from the Ministry of Economic Affairs and Employment) and hosted by the Finnish Radiation and Nuclear Safety Authority (STUK). It had been planned to conduct the mission in October 2020, but due to the COVID-19 pandemic the mission was postponed to 2022. The preparatory meeting was conducted in January 2020 to discuss objectives, scope and other arrangements related to the preparation and conduct of the mission.

For this IPPAS mission, the IAEA assembled a team comprising nine nuclear security experts and a legal expert. These experts have broad experience in nuclear security system design, implementation, regulatory oversight and nuclear security legislation. The IPPAS mission team members were from: Switzerland; Belgium; Canada; Czech Republic; France; Hungary; Japan; United Kingdom; United States of America and IAEA (see also Appendix 2).

(Public) Before the mission, the IPPAS team received a comprehensive Advance Information Package (AIP) provided by STUK. This package included a list of national legislative documents relevant to nuclear security, information about Olkiluoto Nuclear Power Plant (NPP) and the main legislative documents relating to the nuclear security regime, as well as information about Finnish organizations involved in nuclear security. The IPPAS team regarded this as very useful information. The IPPAS team would like to acknowledge Finland's efforts in supporting an IPPAS mission during the time of a global pandemic (COVID-19). These efforts of the host country demonstrate a strong commitment to the security of nuclear and other radioactive material and associated facilities and activities.

(Public) The IPPAS team gathered additional information on the national nuclear security regime through a series of briefings and interviews with officials from STUK as well as other relevant authorities, such as Ministry of the Interior, National Police, Border Guard and the Finnish Security and Intelligence service.

(Public) The IPPAS team also visited Olkiluoto 3 NPP, operated by Teollisuuden Voima Oyj (TVO) and observed the current security practices in place at this nuclear facility. The IPPAS team also visited Turku University Hospital Laboratory (Tykslab) (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]. The meetings at STUK and visits to facilities also provided an opportunity for the exchange of information on international nuclear security practices.

I.1 Objectives

(Public) The objectives of the mission were to:

- Conduct a review of the current status of the national nuclear security regime for nuclear and other radioactive material and associated facilities and activities, and compare it with:

[REDACTED]

- the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment,
 - Code of Conduct on the Safety and Security of Radioactive Sources (CoC),
 - the IAEA Nuclear Security Series (NSS) No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision5),
 - the IAEA NSS No. 14 Nuclear Security Recommendations on Radioactive Material and Associated Facilities,
 - other relevant NSS guidance documents.
- Conduct a review of the implementation of nuclear security at Unit 3 of Olkiluoto NPP,
 - Conduct a review of nuclear security measures at Tykslab [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)
 - Provide advice regarding further enhancement of the national nuclear security regime,
 - Identify good practices that could be communicated to other Member States of the IAEA for long term improvement.

I.2 Scope

[\(Public\)](#) The scope of the mission covered four IPPAS modules: Review of the National Nuclear Security Regime for Nuclear Material and Nuclear Facilities (Module 1), Nuclear Facility Review (Module 2), Security Radioactive Material, Associated Facilities and Associated Activities (Module 4) and Computer Security (Module 5).

[\(Public\)](#) The national level assessment included a review of the legislative and regulatory framework for nuclear security of nuclear and other radioactive material and associated facilities and associated activities, including transport of radioactive material and computer security, as well as regulatory practices (licensing, inspection and enforcement) and coordination between organizations involved in nuclear security.

[\(Public\)](#) The facility level assessment included a review of the current status of the physical protection systems in place at the Olkiluoto 3 NPP. The review was based on the information provided in briefings by the operator, as well as on direct observation of the implementation of physical protection measures during very informative walk downs throughout the facility.

[\(Public\)](#) Nuclear security arrangements [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) were reviewed at Tykslab.

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

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

(Public) Finland is a sovereign unitary state with a well-established constitutional parliament democracy where the powers of the State are vested in the people who are represented by the Parliament. Finland have a classic separation of powers and its legal system is based on written law where the principal areas of law are codified. Since 1995 Finland is a part of the European Union, therefore, the law of EU and EURATOM is also a part of its legal system.

II.1 Legislative Branch

(Public) According to the Finnish constitution (11.6.1999/731, entered into force in 1 March 2000) which is the basis of all legislation and exercise of government power, the legislative power is vested in the Parliament in conjunction with the President of the Republic (sections 3 and 79). The Parliament of Finland (unicameral) decrees the laws while the Government prepares the legislative proposals and undertakes the fulfilment of Parliamentary decisions. Law must be signed by the President and certified by the relevant ministry. Legislative bills are drafted by the Government and prepared by the ministries. Draft bills emanate from the ministry with responsibility for the matter in question. In Finland, there are 12 ministries with a tradition of substantial ministerial independence in the drafting of laws. The ministry responsible for preparing the legislative drafts in the field of nuclear security is the Ministry of Economic Affairs and Employment (MEAE) which is responsible for the overall management and regulation of the nuclear energy sector. In addition, the Ministry of Social Affairs and Health (MSAH) has supreme authority in supervising compliance with the Radiation Act (859/2018) and is responsible for preparing the legislative drafts in the radiation safety sector. The IPPAS team was informed that in practice, drafts of laws and decrees in the civil nuclear energy and radiation safety sectors are formulated in cooperation by the ministries and STUK. This is also derived from the Decree on Finnish Radiation and Nuclear Safety Authority 27.6.1997/618, section 1 (8) which empowers STUK to make proposals for the development of legislation in its field of competence. The IPPAS team was informed that the Nuclear Energy Act (11.12.1987/990) (NEA) is undergoing a complex revision and STUK is currently in early stage of collecting inputs and considering potential amendments to this act.

(Public) According to section 54 of the NEA, the MEAE arranges the self-assessment of the national framework for nuclear safety once every 10 years and invite an international peer review of the national framework of nuclear safety. STUK is also obliged to conduct a self-assessment of its operations relating to nuclear safety. The MEAE would also arrange international peer review of the nuclear safety of nuclear facilities in the event of an accident for which the consequences are significant from the point of view of radiation protection or nuclear safety.

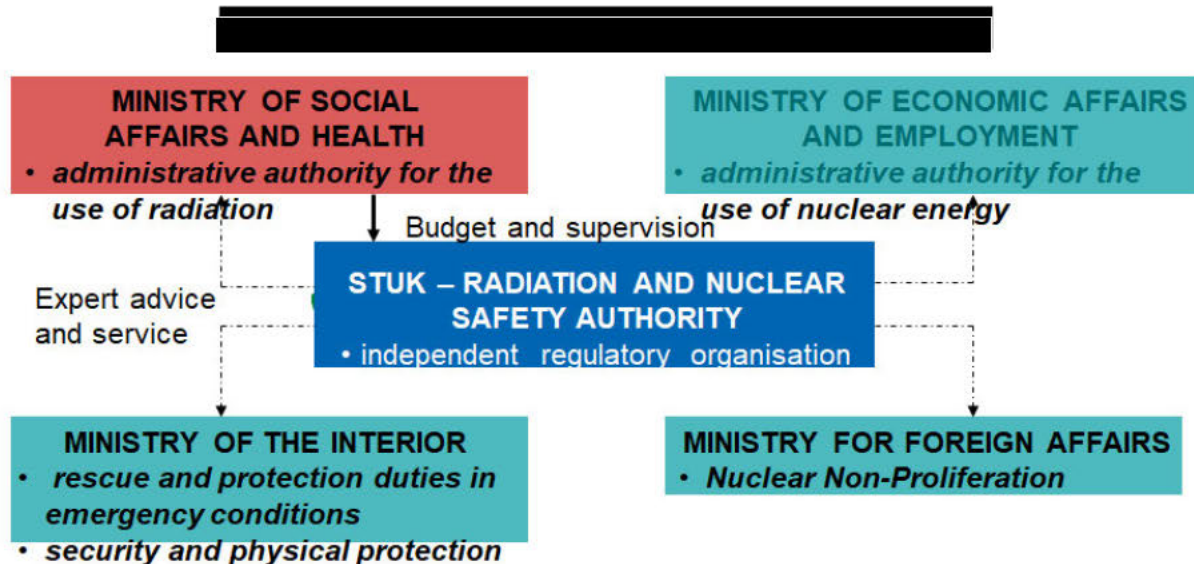
II.2 Executive Branch

(Public) The executive branch in Finland, which directs Finnish politics and is the main source of legislation proposed to the Parliament, is led by the Finnish Government. The Government has collective ministerial responsibility and currently comprises of 19 ministers leading 12 ministries. The leader of the Government is the Prime Minister of Finland. The President of Finland has also a role in the executive branch and works in cooperation with the Government.

(Public) The MEAE is, according to the NEA, the authority responsible for the overall management and regulation of the civil nuclear energy sector. The MEAE is responsible for implementation of energy policy, the objective of which is to consistently progress towards a sustainable climate-neutral society and to promote new energy solutions and their worldwide export. The MEAE has the overall command and control of nuclear energy matters and is in charge of the licencing procedure and preparation of licenses (section 23 of the NEA). License, which is prepared by the MEAE, is in the final stage of being issued by the Government (in case of a nuclear power plant, the Government grants the construction licence, operating licence and decommissioning licence). And before the final decision on the granting of the license, the application is independently assessed by STUK and the assessment (statement) is then made public. The IPPAS team was informed that the Government may decide against the assessment performed by STUK. The fundamental principle D of the Amended Convention on Physical Protection of Nuclear Material (CPPNM/A) requires that the State should take steps to ensure an effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy. Therefore, the MEAE is in charge of the promotion of nuclear energy and for conducting the licensing process but the IPPAS team considers that independent assessment of STUK provides sufficient guarantee for fulfilment of this fundamental principle.

(Public) Other authorities with executive powers who have responsibilities in nuclear security are the police, rescue authorities, and the Finnish Border Guard (including the Coast Guard), all governed by the Ministry of the Interior, the Finnish Defence Forces and Ministry of Defence, the Customs, and the Ministry of Foreign Affairs who has the lead in issues concerning international conventions and agreements (also MEAE participates in negotiations on international agreements and controls and monitors the implementation of the international agreements in this sector).

(Public) The police are responsible for the off-site response at nuclear facilities during security events. In such events, other authorities (including the Finnish Border Guard, Finnish Defence Forces, rescue department) as well as the facility's security organization operate within the joint command-and-control structure, which is led by the police, and may provide their forces and equipment. Coordination and roles of all departments and agencies which contribute to nuclear security is detailed in Chapter IV.3.

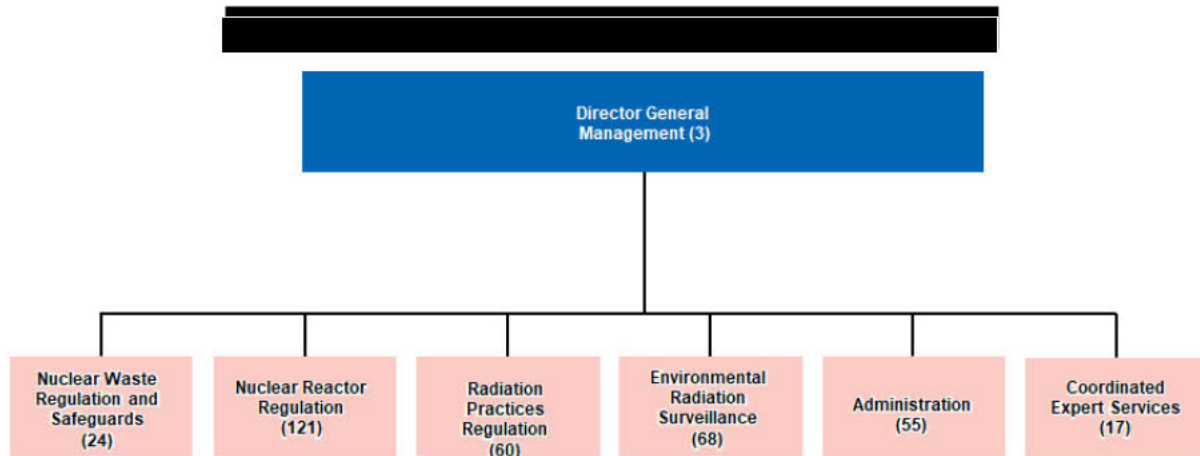


(Public) Fig. 1: STUK and Ministries

(Public) STUK is the regulatory (competent) authority which falls under the jurisdiction (regarding the budget and overall supervision of STUK activities) of the MSAH. The MEAE is responsible for the overall management and regulation of the nuclear energy sector. STUK was originally founded in 1958 and since then STUK has taken on more responsibilities. In the 1980s STUK became the regulator for the nuclear energy sector and begun to conduct the inspections of nuclear power plants. STUK is divided into six main departments:

- Nuclear Reactor Regulation (YTO),
- Nuclear Material and Waste Supervision (YMO),
- Environmental Radiation Surveillance (VALO),
- Radiation Practices Regulation (STO),
- Administration (HAL),
- Relatively recently STUK has also established a new department, Coordinated Expert Services (APA), which cooperates with all the departments of STUK regarding the preparedness, communications, public relations and international cooperation, management and development.

(Public) STUK has currently around 330 employees and the Section for Nuclear Security (YTS) which has currently 6 employees (section head + 5 experts) is located in YTO department. STUK has recently moved its headquarters into a modern building in the city of Vantaa.



[\(Public\)](#) Fig. 2: STUK – Organizational Structure

[\(Public\)](#) STUK issues, maintains and develops nuclear security requirements in the form of binding regulations, regulatory guides and the Design Basis Threat (DBT). According to the NEA, section 23 a statement on the licence application shall be requested from STUK. Even though there are no specific explicit provisions on the independence of STUK, the IPPAS team considers that, for the following reasons, STUK is a well-established and independent regulatory authority:

- STUK is defined and its powers are enumerated by the Act on Finnish Radiation and Nuclear Safety Authority and the NEA. Impartiality and independence of decision-making is ensured through the general administrative legislation (Administrative Procedure Act),
- STUK possesses efficient and effective supervisory powers (e.g. if the use of nuclear energy by an operator is not safe or secure, the activities may be suspended by STUK; STUK conducts independent assessment of safety and security arrangements prior to the authorization of activity; performs independent inspections, may assess required information, impose administrative coercive measures...), and
- STUK has a budget for its regulatory activities which is partially covered by the charges payable to the State (according to the Act on Criteria for Charges Payable to the State, 150/1992 and section 53a of the NEA).

[\(Public\)](#) In addition to these findings, according to the Finnish legislation, the responsibility of nuclear safety and security still lies with the license holder as stipulated in the NEA, Section 7f and nuclear security shall be ensured during the whole lifecycle of a nuclear facility.

II.3 Judicial Branch

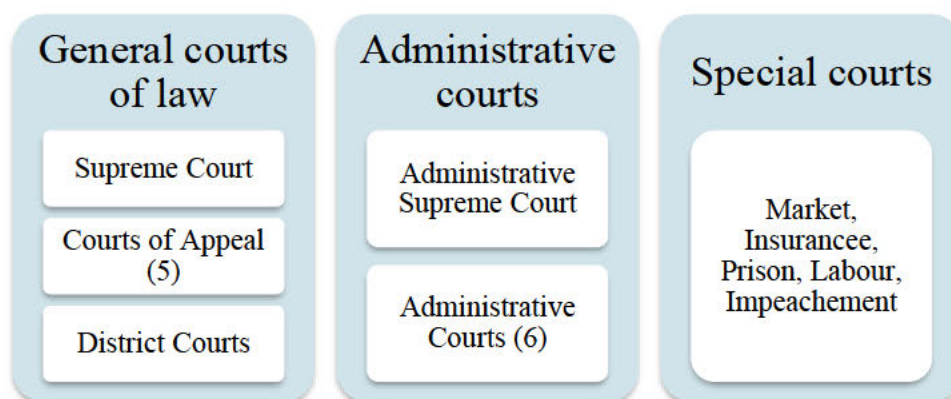
[\(Public\)](#) Judicial power in Finland is vested in the independent courts of law. Chapter 9 of the Finnish Constitution deals with the independence of these courts. Judges are named by the President of the Republic. The first stage of court is the district court and a plaintiff has a right to appeal a decision made in the district court to the court of appeal in order to alter the judgement. If the court of appeal cannot solve the case, the Supreme Court will finally give its judgement for the case. The Administrative courts and the Supreme Administrative Court are entitled to the cases related to administration.

[\(Public\)](#) The role of the courts in nuclear security is mainly supportive. Courts in Finland are responsible for imposing a sentence in criminal proceedings under the Criminal Code of Finland 39/1889 and administrative courts have also a competence to abrogate administrative decisions of public authorities, including administrative decisions made by STUK and the MEAE. This means that STUK's decisions

may be appealed by the independent courts of justice. The IPPAS team was informed that courts may change STUK decision (but these situations are very rare). In case the court decides STUK decision is not appropriate, it will return the case back to STUK for re-assessment. Moreover, the prosecutor shall request an opinion or statement from STUK prior to bringing charges for offences enumerated in the NEA and Radiation Act (section 74 of the NEA and section 184 of the Radiation Act). In Finland this expertise opinion is provided by STUK prior to bringing charges.

(Public) Good Practice 1: The law requires the prosecutor to request an opinion from the regulatory body prior to bringing charges for offences enumerated in the nuclear and radiation legislation before the court of law.

(Public) This is considered as a good practice because offences related to nuclear energy and radiation protection are very rare and in order to prosecute properly, prosecutors and judges need support from subject matter experts.



(Public) Fig. 3: Finnish Courts of Law

(Public) These facts result in the conclusion that the judicial branch of power provides for an effective, well-informed and independent review of the decisions made by the executive branch, including the decisions made by STUK and the MEAE.

II.4 Safety, Security and Safeguards in Finland

(Public) The responsibility for regulatory control of nuclear safety, radiation safety and nuclear security, as well as the national nuclear safeguards/ Nuclear Material Accounting and Control (NMAC), have been vested in STUK (section 55 of the NEA). The fact that STUK is responsible for all three branches of nuclear law provides an opportunity to manage safety/security/safeguards issues in a complex and integrated way.

(Public) Safety, security and safeguards interface is considered during the joint safety and security exercises, document handling, licensing activities (safety, security and environmental protection requirements are met) and inspections. STUK conducts all the inspections related to the safety, security and safeguards of nuclear material and nuclear facilities. According to the YVL A.11 608 also methods of exercises take into account safety accidents and security threats. According to Y/3/2020 chapter 2, section 3 security arrangements shall be consistent with the operation, fire safety and emergency response arrangements of nuclear energy. The objectives of nuclear safeguards and coordination of the

arrangements shall be taken into account in the planning and implementation of security arrangements. Moreover, STUK developed the HAKE system which serves as a database for the inspections conclusions from all safety/security and safeguards areas. Conclusions in the system are regularly evaluated.

(Public) The IPPAS team was informed that STUK supervises the safety culture (including security) of the license holders and the principal approach in Finland is that safety culture covers all domains: safety, security, and safeguards. The topic of integration of security culture into the safety culture is more thoroughly addressed in chapter VII.1 and the topics of the safety/security terminology is addressed in chapter III.2.

III. LEGISLATIVE AND REGULATORY FRAMEWORK

(Public) Finland established a comprehensive framework for the physical protection of nuclear materials and nuclear facilities which is represented mainly by the NEA and implementing regulation Y/3/2020 STUK Regulation on the Security in the Use of Nuclear Energy. STUK is the independent regulatory authority and MEAE is responsible for the overall management and regulation of the nuclear energy sector. There are also other public authorities which are responsible for certain tasks regarding the physical protection of nuclear materials and nuclear facilities.

III.1.1 International Instruments

(Public) Finland is a party to all relevant international conventions on the civil use of nuclear energy and ionizing radiation. Specifically, the following nuclear law and international conventions were ratified by Finland:

- Convention on Nuclear Safety,
- Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management,
- EURATOM Treaty,
- Treaty on the Non-Proliferation of Nuclear Weapons,
- Comprehensive Nuclear Test-Ban Treaty,
- Convention on Early Notification of a Nuclear Accident,
- Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency,
- The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR),
- The Convention concerning International Carriage by Rail (COTIF) annex B (CIM),
- Radiation Protection Convention,
- Paris Convention on Third Party Liability in the Field of Nuclear Energy,

- Brussels Convention Supplementary to the Paris Convention,
- Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention, and
- other bilateral and multilateral conventions regulating the exchanging of information and assistance.

(Public) More specifically, regarding nuclear security, Finland has ratified and implemented the following international instruments:

- Convention on the Physical Protection of Nuclear Material,
- Amendment to the Convention on the Physical Protection of Nuclear Material,
- International Convention for the Suppression of Acts of Nuclear Terrorism, accepted by Finland in 2009,
- United Nation Security Council Resolutions 1540 and 1373.

(Public) Finland is a party to the Convention on the Physical Protection of Nuclear Material (accepted and entered into force in 1989) and deposited its instrument of acceptance to the Amendment to the Convention in June 2011, which then entered into force by national legislation in 2016. Finland submitted the information of their national laws and regulations pursuant to Article 14.1 of CPPNM/A on 6 February 2020 (date of the last submission). The IPPAS team ascertained that some of the information in the submission is already outdated (Regulation STUK Y/3/2020 repealed STUK Y/3/2016). In accordance with Article 5 of the CPPNM/A, Finland has provided the information through the IAEA regarding the national point of contact for nuclear security (STUK). At this point, the IPPAS team concludes that Finland ratified all of the important documents addressing the physical protection of nuclear material and nuclear facilities and plays an active role on an international level.

(Public) Regarding the relationship between Finnish national law and international law, the Finnish legal system is dualistic which means that all international obligation needs to be implemented into the national legislation in order to be binding for individuals and to be enforceable by the public authorities (section 95 of the Constitution). Since the last IPPAS mission, an amendment to the CPPNM came into force internationally. Due to this, the IPPAS team concentrated its work on the implementation of the CPPNM/A and its integration into the national legislation of Finland.

(Public) According to the Decree on Finnish Radiation and Nuclear Safety Authority (27.6.1997/618), STUK is responsible for overseeing the safety, security, preparedness and use of nuclear energy and nuclear materials. Besides that, in accordance with the NEA, the MEAE is responsible for the overall management and regulation of the nuclear energy sector. Under the same act, STUK is responsible for attending to the oversight of security and emergency arrangements and for the necessary control of the use of nuclear energy to prevent proliferation of nuclear weapons. Finland therefore established a competent authority responsible for the implementation of the legislative and regulatory framework according to Article 2A section 2 para b) of the CPPNM/A and as it is described in chapter IV. Finland established and maintains a legislative and regulatory framework to govern physical protection according to Article 2A section 2 para a) of the CPPNM/A. Implementation of fundamental principles according to Article 2A section 3 of the CPPNM/A is analysed and evaluated in the following chapters of this report and possible suggestions for examples of good practices are given there.

(Public) Article 2A para 4 b) of the CPPNM/A requires that nuclear material which, according to the State, does not need to be subject to the physical protection regime, should be protected in accordance with prudent management practice. Even though there is no explicit provision addressing this kind of nuclear material in legislation, provisions in the Section 4 of Y/3/2020 provides sufficient requirements for physical protection of this material and therefore the IPPAS team considers that this provision of the CPPNM/A is fully implemented into the Finnish national legislation. Finnish legislation also does not explicitly address the term *sabotage* but the IPPAS team concludes that the general provisions (basis of security) of the Y/3/2020 provides a sufficient legislative framework to achieve the same objective as it is present in the CPPNM/A.

(Public) Article 3 of the CPPNM/A stipulates that each State Party shall take appropriate steps, within the framework of its national law and consistent with international law, to ensure as far as practicable that, during international nuclear transport, nuclear material within its territory, or on board a ship or aircraft under its jurisdiction insofar as such a ship or aircraft is engaged in the transport to or from that State, is protected at the levels described in Annex I. Annex I of the CPPNM/A further refers to Annex II which contains the table of categorization of nuclear material. Since nuclear material is defined in section 3 of the NEA as special fissionable material and source material, such as uranium, thorium and plutonium, suitable for obtaining nuclear energy and there is no other provision in Finnish national legislation (nor act or regulation) which provides the basis for categorization of nuclear material into the three categories according to Annex II of the CPPNM/A, the IPPAS team would consider it appropriate to transfer the table and the rules for categorization of nuclear material which are currently in the Guide YVL A.11 Security of a nuclear facility 12.02.2021, para. 904 into the official legally binding document - for example the NEA. According to the Constitution of Finland all international treaties need to be implemented into the national legislation in order to be legally binding and enforceable for individuals (including licensees). The CPPNM and its amendment were incorporated into Finnish law through the Decree on the implementation and application of the CPPNM (72/1989) and Government decree on the implementation of the Amendment to the CPPNM and on the entry into force of the Act on the implementation of the provisions of a legislative nature in the Amendment to the CPPNM (338/2016 and 20/2016). However, these are only legal documents which introduces CPPNM/A into the national legislation and due to the fact that provisions of CPPNM/A are not self-executive (stipulates requirements for the State and not for individuals). It further states that Article 3 of the CPPNM/A ("State Party shall take appropriate steps..."), they still need to be substantially implemented into the national legislation. Article 15 of the CPPNM/A stipulates that the Annexes constitute an integral part of this Convention. Therefore, categorization of the nuclear material as provided in Annex II in connection with Article 3 of the CPPNM/A is also required to be enacted by law. The IPPAS team is aware of the fact, that this IPPAS mission does not cover IPPAS Module 3 (Transport Review). The IPPAS team conclude that Finland have not implemented the CPPNM/A properly in case of Article 3 and Annex II of the CPPNM/A (Article 3 of the CPPNM/A refers to the Annex I which refers to the Annex II) but do not make any recommendation regarding this topic.

(Public) In addition to CPPNM/A, NSS 13 also requires that, for protection against unauthorized removal, the State should regulate the categorization of nuclear material in order to ensure an appropriate relationship between the nuclear material and the physical protection measures. The primary factor in determining the physical protection measures against unauthorized removal is the nuclear material itself. NSS 13 provides the table for categorization of 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. As mentioned above, there is no provision in the legally binding document (regarding the legal status of STUK guidelines see chapter III.1.3) which provides the basis for categorization of nuclear material.

(Public) Basis NSS No. 13, para 3.44: “For protection against unauthorized removal, the State should regulate the categorization of nuclear material in order to ensure an appropriate relationship between the nuclear material of concern and the physical protection measures.”

(Public) NSS No. 13, para 4.5: “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.”

(Public) Recommendation 1: The State should amend the necessary legislation in order to implement into the national legislation the categorization of nuclear material in line with NSS 13.

(Public) The criminal offences described in paragraphs (a) and (e) of Article 7 of the CPPNM/A are recognised in Section 69 of the NEA, and punishable under Chapter 34, 44 and 48 of the Criminal Code of Finland 39/1889. The offences described in paragraphs (b), (c) and (f) are punishable under more general Chapters 28 and 31 of the Criminal Code. The offence under the paragraph (d) is punishable under Chapter 34, 44 and 46. Finally, the offences described in paragraph (g) are punishable under Chapter 34(a). In addition, the Criminal Code includes a general provision in Chapter 44 Article 10 on less grave punishable acts relating to the unlawful use of nuclear energy and a provision on punishable acts relating to nuclear explosives in Chapter 34, Article 9. An attempt to commit any of these offences and all forms of complicity are also punishable under Chapter 5 of the Criminal Code. The following table summarizes the implementation of all the relevant provisions in Article 7 of the CPPNM/A into the national legislation of Finland.

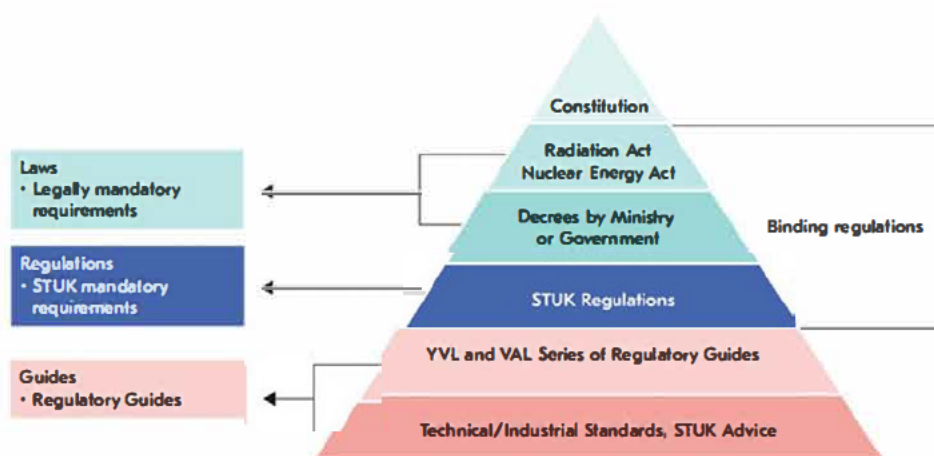
CPPNM/A provision	Criminal Offence	Criminal Code of Finland
Article 7 (1) a)	act without lawful authority	Chapter 34, 44 and 48
Article 7 (1) b)	theft, robbery	Chapters 28 and 31
Article 7 (1) c)	embezzlement, fraud	Chapters 28 and 31
Article 7 (1) d)	carrying, sending or moving NM	Chapter 34, 44 and 46
Article 7 (1) e)	sabotage against NF	Chapter 34, 44 and 48
Article 7 (1) f)	threat, use of force, intimidation to demand NM	Chapters 28 and 31
Article 7 (1) g)	threat to cause damage or to enforce some action	Chapter 34(a)
Article 7 (1) h)	attempt	Chapter 5 and Chapters above
Article 7 (1) i)	participation	Chapter 5
Article 7 (1) j)	organization	Chapter 5
Article 7 (1) k)	contribution	Chapter 5

(Public) *Table 1: Criminal offences and Finnish legislation*

(Public)Based on this analysis the IPPAS team considers that all criminal offences in the CPPNM/A are also punishable according to Finnish national legislation and the CPPNM/A is properly implemented in this regard. Except the abovementioned recommendation, the IPPAS team recognise that the CPPNM/A is properly implemented into the national legislation of Finland.

III.1.2 Laws and Secondary Legislation

(Public)At the top of the legal hierarchy (see fig. 4) of Finnish law is the Constitution which contains fundamental rules concerning the separation of powers (legislative, executive, judicial), contains a list of basic rights and liberties, rules for basic functions of the state and also establishes the general basis for the enactment of nuclear legislation. The Constitution also contains the fundamental principle which requires that the exercise of powers must always be based on law.



(Public) *Fig. 4: Legislative pyramid in Finland*

(Public)The legislative tier consists of acts and decrees issued by the president, by the government or by the ministries.

(Public)The NEA and Radiation Act are the two main acts that set out the legally mandatory requirements relating to nuclear and radiation practices. The Act on Finnish Radiation and Nuclear Safety Authority (22.12.1983/1069) serves as a fundamental basis for the functioning of STUK as a regulatory authority with the power to supervise the use of radiation and nuclear energy, to conduct research and education and to inform others about these topics.

(Public)The Criminal Code of Finland (39/1889) enumerates punishable offences which incorporates the provisions in CPPNM/A while it determines the conditions for criminal liability, particular offences and sets imposable punishments.

(Public)The Private Security Services Act (1085/2015) stipulates general requirements for the nuclear security officers. These requirements are significantly complemented by the provisions in the NEA (section 7m and following sections).

(Public) The Police Act (872/2011) in relation to the NEA (section 68) specifies the role of the police as a response force during nuclear security events at nuclear facilities and legally establishes the police's other responsibilities and roles.

(Public) The Act on Background Checks (726/2014) which entered into force in 2015 stipulates the procedures to be applied in order to verify the reliability of persons and companies (security vetting by the Finnish Security and Intelligence Service (SUPO)) with the intention to reduce the vulnerability of society and to protect public interests, including national security, national defence interests and public safety.

(Public) The Act on the Openness of Government Activities (21.5.1999/621) stipulates that everyone has a right to obtain public information from official documents and those documents are public unless specified otherwise and classified in accordance with the Act (section 10). Detailed provisions regarding the public availability of the information connected to nuclear facilities are given by section 24 of this Act.

(Public) The general administrative legislation creates the link between the Constitution and substantive legislation represented by the NEA. The general administrative legislation addresses administrative procedures, openness of governmental activities, information management in public administration, data protection, conditional fines and other administrative enforcement which is applicable to STUK and to the MEAE activities.

(Public) Since the 2009 IPPAS mission and 2012 follow-up IPPAS mission, Finland has significantly amended the NEA and the Government Decree on the Security in the Use of Nuclear Energy. Additionally, the amendment of the decree in April 2012 incorporated new provisions regarding the training and use of firearms and other weapons by nuclear security officers. Another significant change to the legislation regarding nuclear security was introduced in 2020 by the Act no. 11.12.2020/964. During its existence, the NEA has already been amended 30 times. The most important amendments to the NEA from 2020 deal with preparing for the new threats (e. g. drones, a doctors right to notify the license holder, STUK and other authorities about medical conditions of individuals) and implementing the latest international recommendations and other legal rules. To emphasize that nuclear security officers at nuclear facilities have greater rank and powers than private guards, and to ensure that these nuclear security officers would be competent and adequately equipped to provide a response in case of a nuclear security event, Finland incorporated into their national legislation detailed provisions regarding the powers, competencies and equipment of nuclear security officers. This includes the right to prevent access to the nuclear facility area, to remove a person from the nuclear facility area and to remove from a person any material or object suitable for harming a person or property. It also includes the authority to take temporary possession of an remotely piloted aircraft system by using a technical device or force, to prevent its use or otherwise intercept it if the remotely piloted aircraft system unlawfully enters an area in permanent use by the licence holder where aviation is prohibited.

(Public) Good Practice 2: There is a clear, detailed and extensive list of competencies, rights and powers of nuclear security officers in national legislation including the right to take action against the use of an remotely piloted (or programmed) aircraft system (RPAS).

(Public) The IPPAS team was informed that in Finnish the same word "*turvallisuus*" for both *safety* and *security* is used. This fact may cause some uncertainties regarding the interpretation of legal texts which regulates nuclear safety and security. Section 3 (6) of the NEA defines *security* (*turvajärjestelyillä*) as *the security arrangements needed to protect the use of nuclear energy against activities endangering*

nuclear or radiation safety at the nuclear facility and in its area and on other sites or vehicles where nuclear energy is used. Further provisions which deal with the security arrangements are incorporated in section 7l of the NEA and these provisions operate with the word “*turvajärjestelyt*”. When describing the powers of the nuclear security officers in section 7m, the NEA uses the term “*turvahenkilöt*”.

(Public) In other instances, the NEA uses the term “*turvallisuus*” with the intention to address both safety and security. The IPPAS team was informed that in some cases this term reflects both safety and security but in other cases (depending on the context or on the implementing legislation) this term may refer only to nuclear safety. The IPPAS team was also informed that an ordinary native Finnish speaker would not be aware of a different meaning of the word “*turvallisuus*” in the written legislative text. For example the fact that nuclear safety culture also comprises the nuclear security is only further clarified in the Guide YVL A.11 Security of a nuclear facility 12.02.202 section 408 which stipulates that “*Safety culture as a term also covers nuclear security.*” Another example is section 7r which authorizes STUK to specify detailed safety requirements concerning the implementation of safety levels in accordance with the NEA and this provision uses only the term “*turvallisuus*” which is translated as *safety*. On the other hand, section 7q in the list of matters where STUK is empowered to issue regulations explicitly mentions the planning of the security arrangements in the use of nuclear energy (see also Chapter III.1.3). Furthermore, it is not entirely clear if section 54 of the NEA, which requires MEAE self-assessment of the national framework of nuclear safety, also comprises the self-assessment of the national framework of nuclear security or if STUK is empowered to include in its statement a proposal for licence terms which are necessary in order to implement the security requirements according to section 23 of the NEA. In order to ensure that security measures do not compromise safety and safety measures do not compromise nuclear security, the IPPAS team finds it appropriate to clarify the distinction between safety and security and to have straight-forward security-specific terminology when referring only to security matters. Finland should then consider amending the relevant legislation to clearly define the two separate concepts of safety and security. As previously mentioned, the IPPAS team was informed that STUK is currently considering a revision of the NEA. Thus revision would provide an opportunity to address the issue of specific safety and security terminology.

(Public) Basis NSS No. 20, para 1.2: “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.”

(Public) Recommendation 2: To eliminate the ambiguity and to ensure that security measures do not compromise safety and safety measures do not compromise security, legislation should clearly express which cases address only *safety*, which cases address both *safety* and *security* and which cases address only *security* issues.

(Public) The IPPAS team noted that definition of nuclear security in the section 3 (6) of the NEA does not consider the security of other radioactive material whereas other documents (e.g. guides, DBT) encompass it. Also the IPPAS team noted during its extensive discussion with STUK that nuclear security in regulatory practice encompass also the other radioactive material. The IPPAS team observes a discrepancy between the legal terminology and practice in this regard.

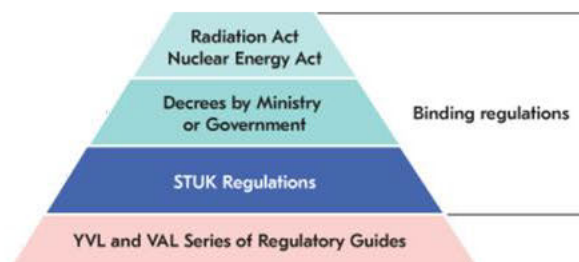
(Public) On the decree level, the Nuclear Energy Decree (NED), which encompasses nuclear safety, nuclear security and NMAC, the Decree on Finnish Radiation and Nuclear Safety Authority

(27.6.1997/618), which relate to the tasks of STUK and Government Decree on Security Classification of Documents in Central Government (1101/2019) are also relevant.

III.1.3 Regulations and Technical Guidance

(Public) On the next implementing tier of the legislative pyramid are the STUK regulations (regulating issues which were previously regulated by the Government Decrees), underneath which are STUK regulatory guides.

(Public) As of 2015, STUK possess the competence to issue binding regulations, which are positioned between the legislation and the regulatory guides in the legislative and regulatory framework. Competence to issue regulations in the area of nuclear security is derived from section 7q (21) of the NEA which determines that STUK issues further regulations on the technical details of the principles and requirements laid down in the NEA. These concern the planning of the security arrangements in the use of nuclear energy, their implementation, personal security, information/cyber security, security control, the uniform of the nuclear security officers, security standing orders, preparedness for threats and actions during a threat and the marking of an area of restricted movement in a nuclear facility. Therefore, the former Government Decree on the Security in the Use of Nuclear Energy was replaced by STUK Regulation on Security in the Use of Nuclear Energy, which entered into force in 2016 as a STUK Y/3/2016. The latest version of this regulation entered into force in 2020 as the STUK Regulation on the Security in the Use of Nuclear Energy Y/3/2020.



(Public) Fig. 5: Implementing regulations and guides

(Public) The right to issue the regulations is not covered explicitly in the Constitution of Finland but it is based on section 7q of the NEA which enables STUK to issue and publish these technical requirements. This is according to Constitution of Finland, Section 80, which allows the competent authority to stipulate regulations, if that power has been assigned in the Act for such authority. Prior to issuing the regulations STUK shall hear the views of the license holders, the Advisory Commissions referred to in section 56 of the Nuclear Security Act, the Ministry of the Interior, the Ministry of the Environment and the rescue authorities as well as other authorities as appropriate. Also, according to section 1 (8) of the Decree on Finnish Radiation and Nuclear Safety Authority (27.6.1997/618), STUK is legally authorised to make proposals for the development of legislation in its field of competence and provide general guidance on radiation and nuclear safety.

(Public) Implementing Y/3/2020 STUK Regulation on the Security in the Use of Nuclear Energy applies to security arrangements in the use of nuclear energy. This regulation specifies requirements applicable to a licensee concerning the implementation of security arrangements and applies to a nuclear facility at different points of its life cycle and to the transportation of nuclear material and nuclear waste related to the operation of a nuclear facility. This regulation is also applicable in enumerated cases to other uses of nuclear energy and provides for physical protection and information/cyber security.

(Public)Based on section 7r of the NEA, STUK issues detailed safety provisions concerning the implementation of safety levels in the form of guides. STUK explained to the IPPAS team that this section also includes considerations relating to nuclear security even though it is not explicitly mentioned in section 7r (in comparison with section 7q). In this regard, STUK issued three guides which are part of the nuclear security framework in Finland:

- YVL A.11 Security of a nuclear facility,
- YVL A.12 Information security management of a nuclear facility,
- Security arrangements of radiation sources guide.

(Public)Other guides that are not primarily dealing with security matters also contain important security provisions such as the following:

- YVL A.1 Regulatory oversight of safety in the use of nuclear energy,
- YVL A.2 Site for a nuclear safety,
- YVL A.4 Organization and personnel of a nuclear facility,
- YVL D.1 Regulatory control of nuclear safeguards.

(Public)In general STUK guides are categorized in accordance with the codes below:

- YVL guides relating to the nuclear facilities,
- B guides relating to the plants and systems designs,
- C guides relating to the safety of nuclear facilities and the impact on the environment,
- D guides relating to nuclear material and nuclear wastes,
- E guides relating to the structures and equipment of nuclear facilities,
- ST guides on radiation safety (not revised anymore).

(Public)According to section 7r (3) of the NEA, the safety requirements of the STUK are binding on the licensee, while preserving the licensee's right to propose an alternative procedure or solution to that provided for in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with this Act, STUK may approve a procedure or solution by which the necessary safety level is achieved. These requirements are published as part of the regulations collection issued by STUK. There is no other provision regarding this regulations collection in the NEA. The IPPAS team were informed that there is currently no legal basis in the Constitution for issuing the legally binding requirements on the guidance level. This concept is also no longer present under the Radiation Act which underwent a complex revision in 2018 and which only enables STUK to issue legally binding regulations (section 67 of the Radiation Act). STUK guidance refers to the provision 7r of NEA and requirements and objectives are not clearly identifiable from the wording of the STUK guidance.

(Public)Moreover, the IPPAS team underlines that the abovementioned suggested solution regarding the terminology issue between *safety* and *security* in the previous chapter III.2. would also be beneficial with regard of the wording of section 7q and 7r of the NEA. Section 7q stipulates that STUK is legally authorised to issue further regulations on the technical details of the principles and requirements laid

down in the NEA and in para (21) explicitly mentions the security arrangements in the use of nuclear energy and section 7r specifies detailed safety requirements concerning the implementation of safety levels in accordance with the NEA with no explicit indication of security arrangements.

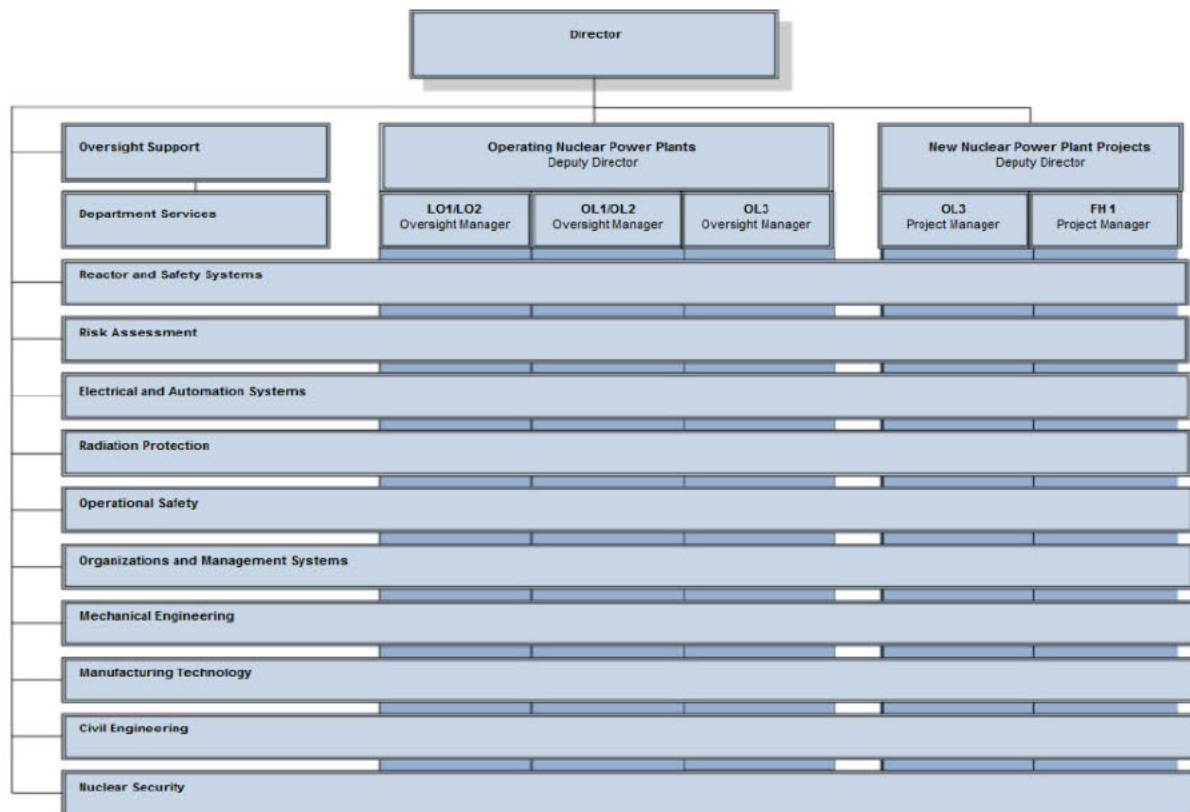
(Public)Basis NSS No. 27-G, para 3.12: “States should develop and implement regulations consistent with the State’s legislative framework. The exact nature and content of regulations will depend on the decisions taken by a State about the manner in which the regulatory function is carried out, including the number of competent authorities involved in supervising the physical protection regime.”

(Public)Suggestion 1: The State should consider revising the enabling clause in section 7r of the NEA with the purpose of clarification the legal status of the guidance documents. In order to do so, the State should consider abrogating this provision and transfer legally binding requirements from guidance documents into the STUK regulations.

IV. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

(Public)STUK is divided into 5 main departments: YTO, YMO, VALO, STO and HAL. STUK has also established a new department, called Joint Specialist Services (APA).

(Public)YTO is in charge of Nuclear Reactor Regulation. It includes a section for nuclear security (YTS).



(Public) Fig. 6: Organizational chart for YTO

(Public) YTS's responsibility is to supervise the security arrangements (including computer/cyber security) of nuclear facilities. YTS will also support other offices and departments of STUK when needed. Each member of YTS has a specialty in a dedicated area such as information and cyber security, legislation, response of security organization etc.

IV.1 Cooperation within STUK

(Public) The IPPAS team was informed that many arrangements within STUK contribute to good cooperation between STUK offices and departments.

(Public) For example, Internal Guide YTV 3.c.5 describes comprehensively what responsibilities each office and department have, how they support each other, and how to ensure good coordination. The IPPAS team had the impression that STUK personnel from YTO, YMO and STO, were fully aligned with these principles.

(Public) The IPPAS team also noted that STUK's nuclear safety inspectors, including resident inspectors, have a basic training in security matters. It allows for synergy regarding inspection findings during nuclear safety inspections. The IPPAS team was informed that this organization had proven to be very useful for Olkiluoto NPP, where the resident inspector provided significant support to YTS for the licensing process regarding nuclear security. In this regard, the IPPAS team found that the HAKE repository database used by STUK to share security findings between inspectors, combined with the monthly analysis of these findings, seemed to be an effective way to take advantage of STUK's organisation taking into account the need-to-know basis.

(Public) Additionally, the IPPAS team was informed that STUK organise exercises involving both safety and security aspects and had the opportunity to visit the new emergency centre. The IPPAS team observed that this new centre provides specific equipment needed for nuclear security assessment in case of nuclear events, including a room dedicated to reach back for detection of materials out of regulatory control, and dedicated offices for nuclear security experts.

(Public) **Good Practice 3:** STUK as the competent authority has established and maintains several mechanisms allowing for close internal cooperation between the STUK's entity in charge of security and STUK's entities in charge of safety and safeguards.

IV.2 Licensing/Authorization Process

(Public) Following the NEA, the construction of nuclear facilities considered to be of considerable general significance, including nuclear power plants, requires different licensing steps during which safety, security and safeguards provisions should be addressed. The following steps need to be considered:

- The government decision-in-principle
- The construction license
- The construction
- The operational license
- The operation

(Public) In addition to these steps, the operator will have to consider, in due time, the introduction of a decommissioning license. Following its reading of the legal and regulatory texts, and discussion with STUK, the IPPAS team noted that nuclear security considerations are taken into account in each of the aforementioned steps. This contributes to supporting a security-by-design approach for the most important nuclear facilities.

(Public) The NEA stipulates that the government or MEAE, depending on the nuclear facility project in question, is the licensing authority. In this regard, STUK is responsible for assessing the safety and security arrangements throughout the whole project and for providing technical statements for the attention of the licensing authority. However, STUK is also the licensing authority for other activities involving nuclear material and nuclear waste such as the possession, manufacture, production, transfer, handling, use, storage, transport and import of nuclear material, unless these activities are performed within nuclear facilities.

IV.2.1 The Decision-in-Principle

(Public) The so-called decision-in principle step is not a licensing stage as such, however it is a major step to be considered for projects relating to nuclear facilities of considerable general significance. During this step, the operator has to demonstrate that the construction project is in line with the overall good of society. An application must be submitted to the government and then the MEAE then receives a preliminary safety assessment from STUK as well as statements from other entities such as the Ministry of the Environment and the neighbouring municipalities. Even before the decision-in-principle, a public hearing is needed. However, the IPPAS team has not been made aware if security concerns would be taken into consideration during the hearing process.

[REDACTED]

(Public) While the NEA does not mention any specific requirement relating to nuclear security during this step, the NED contains a provision on section 24 relating to that and the YVL A.11 guide specifically mentions that in connection with the submission of an application for a decision-in-principle for a nuclear facility, a description of the suitability of the planned location taking into account both security and safety considerations, should be submitted by the operator to STUK. It was understood by the IPPAS team that this documentation provided to STUK is considered in the preliminary safety assessment which the regulatory body prepares and provides to the Ministry of Trade and Industry. Furthermore, the NED and the YVL A.11 mention that during this decision-in-principle step, provisions relating to aircraft crash should be considered.

(Public) Finally, it can be noted that when granted, the government decision-in-principle documentation has to be sent to Parliament for consideration and that Parliament has the authority to reverse the decision to grant the decision-in-principle.

IV.2.2 The Construction License

(Public) The NEA stipulates that a construction license can be granted if, among other things, security has been adequately taken into account during the design phase. The YVL A.11 adds that when submitting a construction license to STUK, a preliminary plan for the security arrangements should also be submitted in accordance with the NED. The aim of this preliminary plan is to present the proposed security criteria, the technical implementation projects relating to security and the demonstration of the adequacy of the proposed security arrangements with the existing requirements and guidance (if applicable). It is during this phase that the operator will also have to submit to STUK a draft security standing order, describing the security provisions relating to the on-site response force and the functioning of the security teams within the site, during the operation of the nuclear facility. The YVL A.11 specifies in section 704a which information should be provided in the security plan, including the following:

- Risk analysis.
- Definition of protection needs and vital areas, design criteria for the security arrangements and a comprehensive description of the design principles and technical solutions.
- A description of the security arrangements for the construction phase of the nuclear facility.

(Public) The aforementioned guide also states that from this stage approval from STUK will be needed for any changes made to the security plan and security standing order and that other documents should be submitted by the operator to STUK for information. This includes a description of how requirements pertaining to nuclear security during operation have been taken into account in the construction and implementation phases. The IPPAS team was also informed that the license applicant must inform STUK about the design basis and auditing programs regarding plant manufacturers, including security considerations. STUK also informed the IPPAS team that during this construction license phase STUK requires a statement from the Ministry of the Interior and the Advisory Commission on Nuclear Security on the adequacy of the security arrangements.

(Public) The NEA also stipulates that nuclear security officers should be used from the moment a construction license is granted.

[REDACTED]

IV.2.3 The Construction

(Public) The IPPAS team was informed that when the construction license is approved, the construction works can begin only after STUK has verified that factors affecting security, based on previous engagement between STUK and the license applicant, have been considered. STUK explained that inspections are conducted during the progress of the construction works.

IV.2.4 The Operational License and the Commissioning phase

(Public) The NEA stipulates that a license to operate can be approved after a license has been granted for construction and after certain conditions have been met; none of these conditions specifically relate to nuclear security. However, the NED and the YVL A.11 specify that an updated security plan, as well as an updated security standing order, should be submitted to STUK for approval during this phase. This updated security plan must contain information relating to how the DBT is addressed by the physical protection system. According to the YVL A.11, other documents must be submitted to STUK for information during this phase including schedules of implementation of various aspects of security arrangements and installation and commissioning of security devices.

(Public) The NEA also states that the operation of the nuclear facility cannot be started on the basis of the operational license granted until, amongst other conditions, STUK has confirmed that the nuclear facility and its physical protection system meet the security requirements. In particular, the IPPAS team was informed that STUK conducts security inspections during the commissioning phase and that during this phase STUK is also required to request a statement from the Ministry of the Interior and the Advisory Commission on Nuclear Security confirming the adequacy of the security arrangements.

(Public) In conclusion, the IPPAS team considered that the licensing and authorization process in Finland does allow for the early consideration of important elements of nuclear security in nuclear facility projects. However, the IPPAS team noted that many important provisions relating to nuclear security during the licensing and authorization process of nuclear facilities are addressed in the security guide YVL A.11.

IV.3 Inspection and Enforcement

(Public) According to the NEA, STUK is entitled to:

- Inspect and control operations relating to nuclear facilities
- Demand that the operators provide access to nuclear facilities when needed for the conduct of its mission
- Receive and request from the operators the necessary information for the conduct of its mission
- Demand the operators submit standard format reports, as well as necessary information and notifications
- Investigate abnormal events or procedures in the use of nuclear energy

(Public) Regarding nuclear security inspections in nuclear facilities, it was mentioned that the internal YTV 4.a.1 and YTV 4.b.1 provide guidelines on how STUK conducts its inspections. However, the content of these documents has not been read by the IPPAS team.

(Public) The IPPAS team was informed that three generic types of inspections can be performed:

- Regular inspections carried out each year and notified beforehand.
- Reactive inspections conducted when a security (or a safety) event has occurred and when it is considered necessary to verify that the operator is complying with its obligations. Such inspections can also be used to investigate the causes of the security event, and to understand how the operator addressed this event.
- Unannounced inspections for which no previous notification is sent to the operator. A reactive inspection can also be an unannounced inspection.

(Public) STUK performs inspections relating to construction permits (RKT inspections), inspections during construction (RTO inspections) and inspections when facilities are operating (KTO inspections). KTO inspections are used to verify that the facilities are operated and maintained according to the legal and regulatory requirements, the DBT and the operators' procedures and rules. STUK considers that the nuclear material inspections either conducted solely by STUK or together with Euratom and IAEA are also an opportunity to check that the NMAC system is in order and that no clandestine action has taken place within the facility or within an inspected non-nuclear facility where nuclear material is used (e.g. a protracted theft of nuclear material). In this regard, it was mentioned to the IPPAS team that YTS also collaborates with the Nuclear Material Section YMA and other sections of the YMO department. YTS provides training to its own inspectors, and basic training and awareness programs to inspectors of other sections. As a result of this wider security awareness programme, inspectors from other sections also have a limited capability to identify and verify security related issues when performing their own on-site inspections. In this regard, it was specifically mentioned by STUK that YMA is responsible for the oversight of the security arrangements of the non-nuclear facilities. Also the IPPAS team were informed that STUK resident inspectors are present at both Loviisa and Olkiluoto NPPs and that these inspectors may conduct security related activities if requested by YTS. STUK highlighted the example of one resident inspector at the Olkiluoto site who was aware of the main security points and issues at the NPP.

(Public) The IPPAS team was informed by STUK that YTS usually conducts one site inspection annually at each of the nuclear sites. For the nuclear power plants, the IPPAS team were informed that approximately a total of twenty man-days was allocated to nuclear security inspections. At OL3, YTS has focused its security inspections in 2021 on security arrangements at the plant gate and on operations at the alarm station (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) It is stated in the NEA that if the provisions relating to safety and security, including those stipulated in the regulations and license conditions are not fulfilled, STUK can issue instructions to the operators to address the defects and/or the defaults within a time period specified by STUK. STUK can also use coercive measures by imposing conditional fines and interrupting or limiting the operation. The interruption or limitation of the operation may be ordered by STUK, in the event of a defect or default which has the potential to result in immediate danger. Such interruption and limitation measures could also be implemented in relation to other conditions laid down in the NEA. This act also stipulates that the public prosecutor shall not bring charges for certain types of offences relating to nuclear security (e.g. provisions on punishment for nuclear device procurement) before obtaining statements on these matters from STUK. Also, upon a request from STUK, police can assist with the conduct of searching premises.

(Public) Based on the aforementioned information, the IPPAS team considered that the inspections conducted at Loviisa and Olkiluoto NPPs allow STUK to perform its duties relating to the nuclear

security oversight of the NPPs. Also the IPPAS team considered that STUK is provided with sufficient enforcement capabilities.

(Public) Overall the IPPAS team found that STUK has established and maintains a comprehensive nuclear security inspection program at NPPs.

IV.4 Coordination with Other State Organizations that Contribute to Nuclear Security

(Public) In the presentations and discussions during the IPPAS mission, the coordination with other State organizations was extensively covered. The following national authorities were presented in more details:

- Ministry of Defence
- MEAE
- Ministry of the Interior
- Finnish Customs
- Finnish Transport and Communications Agency (TRAFICOM) (in charge of security of transports and of computer security)
- Border Guard
- National Police Board
- SUPO (Finnish Security and Intelligence Service)

IV.4.1 Advisory Commission on Nuclear Security

(Public) In particular, the Ministry of the Interior presented on the “Advisory Commission on Nuclear Security”.

This commission is prescribed by the NEA Article 56 stating that “in the handling of matters concerning security during the use of nuclear energy, an advisory committee appointed by the Government works in conjunction with the Radiation and Nuclear Safety Authority (STUK)”.

Duties of this commission are:

- Prepare and issue statements on security assessments and plans
- Issue statements on STUK’s and other authorities’ legislation, orders and guidelines
- Issue statements on other important matters of nuclear security
- Assess the threats to the use of nuclear energy and assess level of preparedness
- Advance domestic cooperation and information sharing and conduct international cooperation
- Make suggestions to competent authorities of necessary actions to enhance nuclear security

This commission is composed of:

- Ministry of the Interior

- 
- MEAE
 - Ministry of Defence
 - National Police Board
 - Local Police Departments
 - Local Rescue Departments
 - Border Guard
 - SUPO
 - Customs

(Public) The operators attend the commission meetings as observers.

(Public) This commission make assessments of the nuclear security of NPPs on a 3-year basis.

(Public) **Good Practice 4:** the Advisory Commission on Nuclear Security is established by the law, supports and provides advice to other competent authorities including STUK. Its duties cover security assessment of nuclear facilities, laws, regulations and guidance, threat assessment, cooperation and suggestions to competent authorities. Operators can attend these meeting as observers.

(Public) Nevertheless, the IPPAS team was informed that the Advisory Commission on Nuclear Security does not have high capabilities regarding computer security, and no similar, formal, commission exists for computer security. For example, TRAFICOM, which is one of the major Finnish stakeholder in this matter, is not part of the commission.

(Public) **Basis** NSS No. 42-G, para I-14: “The State should ensure that functions, roles, and other provisions for computer security are defined and closely coordinated between and within all competent authorities involved in nuclear security.”


(Public) **Suggestion 2:** The State should consider expanding the membership of the Advisory Commission on Nuclear Security and include other authorities to enhance its capabilities to address computer security related issues.

IV.4.2 Practical arrangements with local authorities

(Public) Moreover, during the visit to Olkiluoto NPP, the IPPAS team met local representatives from:

- Defence forces
- Border guard
- Satakunta rescue department
- local police forces

(Public) Based on these presentations and discussions, the IPPAS team noted that Finnish authorities consider coordination between security and emergency authorities and the operator as very important. For example:



- several statements of representatives emphasized the importance of good coordination and cooperation between different stakeholders and considered it was one of the most important strength of Finnish security culture
- a common and secured communication system providing good interoperability between all stakeholders
- common, regular exercises involving authorities (Police, Defence forces...) and the operator
- laws giving clear responsibility to the police to ensure armed response in case of a nuclear security event, and requiring other authorities to give assistance to the police if requested (*Police Act (872/2011) Ch. 9, section 2*, Border Guard, Customs etc.; *Act 781/1980 (under revision), section 1*, Defence Forces)
- police contingency plans are designed in close collaboration with the operator

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

- common system to share security information ("situation picture system") between authorities, including police, STUK, and the operator

(Public) Coordination is also prescribed by nuclear security requirements, such as:

- "The licensee shall specify who will lead the measures to be taken against the threat once the threat has been detected. Section 7 n of the NEA contains provisions concerning the transfer of leadership responsibility for security arrangements to the police under a threat." (*STUK Y/3/2020: Ch 5, Section 12*)
- "The licensee shall provide the police authority with the opportunity to participate in the preparation of security arrangement plans and measures related to threats." (*STUK Y/3/2020: Ch 6, Section 14*)
- "Information on the threat and its progress shall be submitted to the police as early as possible before they arrive at the scene." (*STUK Y/3/2020: Ch. 5, section 12*)
- "The licensee shall appoint a sufficient number of persons with expertise in nuclear safety, radiation safety and security arrangements to assist the police. The licensee shall take care of the matters related to nuclear safety and radiation safety at a nuclear facility." (*STUK Y/3/2020: Ch. 5, section 12*)

(Public) The IPPAS team observed very strong cooperation between the operator and authorities to ensure a high level of coordination for response to nuclear security event.

V. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)

(Public) Finland has established and maintain a DBT for nuclear facilities. According to the NEA, Section 71 (11.12.2020/964) states:

Security arrangements (2nd paragraph): “The security arrangements shall be adequate in relation to the threats involved against in the use of nuclear energy and the need for protection.”

(Public) STUK presented the process of threat assessment, led by SUPO, in cooperation with the National Bureau of Investigation, Defense forces, different national and local police services and the national Cyber Security Centre, prescribed by the NED Section 146.

(Public) Based on that threat assessment and section 146 of the NED, STUK is responsible for issuing the DBT, with the support of the Police Department of the Ministry of the Interior and the Advisory Commission on Nuclear Security. Operators are also requested to provide comments.

(Public) Y/3/2020 Radiation and Nuclear Safety Authority Regulation on the Security in the Use of Nuclear Energy, Chapter 2 “Basis of security”, Section 3 “General planning criteria for security arrangements” states:

“1. The planning of security arrangements shall be based on the design basis threat, the risk analyses of the activity to be secured, and the protection requirements assessed on the basis thereof.”

(Public) STUK presented their DBT methodology and structure and the IPPAS team was able to have very open discussions on that matter. From their observations and discussion, the IPPAS team considers that the Finnish DBT is aligned to NSS No. 10-G (Rev. 1) main recommendations, with some specificities.

(Public) A chart (figure 7) illustrating unacceptable levels of radiological consequences (dose limits in mSv) was shown to the IPPAS team. There are different DBTs for each level of radiological consequences. The figure is applicable to nuclear facilities and transport of nuclear fuel.

Threat levels and dose constraints (mSv)	Threats beyond the design basis threat				
	Extreme sabotage, theft	5	X	Obtaining of nuclear material	
	Airplane crash	4	20		
	Sabotage, theft	3	5 0.1		
	Widescale vandalism, information system disruption, theft	2	0.1		
	Vandalism, influencing through information networks, random theft	1	0.1	Proliferation of sensitive information	Illegal trade in other nuclear commodities and dual-use items
Threat types	Vandalism, sabotage, theft	Level	mSv	Proliferation	

mSv: Annual dose constraint for an individual of the population (not specified for a theft or proliferation threat)

Level 3: Nuclear facility 5 mSv, transport 0.1 mSv

Level 5–X: Over 20 mSv during the first week to an unprotected person – a need for evacuation outside the precautionary action zone must not be created at the nuclear facility, safety distance for an individual of the population must be ensured during transport

Levels 1–5 apply to Class 1 nuclear facilities

Levels 1–3 and 5 apply to transport of spent nuclear fuel

Levels 1–3 apply to Class 2 nuclear facilities

Levels 1–2 apply to Class 3 nuclear facilities and transport of fresh nuclear fuel

[REDACTED]

(Public) Fig. 7: Threat levels of the DBT

(Public) The IPPAS team considers that the process for threat assessment and DBT implemented in Finland, while being relatively new, is comprehensive and mature.

(Public) The IPPAS team was informed that the DBT was revised between 2016-2020. The new DBT entered into force in 2020 for new build nuclear facilities. For existing and nuclear facilities under construction, including Olkiluoto 3 NPP, the DBT applies but with possibilities to give derogations through “implementation decisions” delivered by STUK.

(Public) STUK explained that these implementation decisions take into account the fact that some aspects of design basis threats cannot be addressed for existing facilities, such as [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

(Public) Rules for application of YVL A.11 states “When considering how the new safety requirements presented in the YVL Guides shall be applied to the operating nuclear facilities, or to those under construction, STUK will take due account of the principles laid down in Section 7a of the NEA (990/1987): “The safety of nuclear energy use shall be maintained at as high a level as practically possible”.

(Public) As an example, the TVO operating licence application for a nuclear power plant unit OL3, 2.1 Design bases 3, page 167, states: “The design of the security arrangements is based on the threats that TVO determined in cooperation with the authority before STUK confirmed the design basis threat via its decision 2/Y42217/2013. The original design basis threat, the consideration of which is discussed in the final safety analysis report and its appendices, did not include all of the threats mentioned in decision 2/Y42217/2013. These are taken into account in accordance with Section 7 of the NEA in a manner similar to the application of new YVL Guides. The matter is discussed in more detail in the DBT application assessment.”

(Public) The IPPAS team was informed the such derogations are given after a sound assessment, taking into account the principles laid down in Section 7a of the NEA. Nevertheless, it was said that no systematic approach exists for nuclear security assessment. The IPPAS team recognizes that such assessment require expert opinion. Nevertheless, guidance can be very helpful in clarifying how methods can be used in order to meet performance-based requirements.

(Public) **Basis** NSS No. 27-G, para 4.53: “Several performance based approaches are available to evaluate the effectiveness of the physical protection system against insiders and external adversaries. Performance based evaluation methods include: [...]”

(Public) NSS No. 27-G, para 4.56: “System effectiveness can be measured either quantitatively or qualitatively. The State should decide which approaches should be used for different types of targets, threats and scenarios.”

(Public) **Suggestion 3:** STUK should consider developing guidance to provide for a systematic approach for assessing the effectiveness of nuclear security system.

VI. RISK INFORMED APPROACH

[REDACTED]

VI.1 Risk Management

(Public) While no specific provisions for a risk informed approach to nuclear security are defined in the NEA, the STUK regulation Y/3/2020 provides the basis for such an approach by stipulating that the planning of security arrangements should be based on the DBT, the risk analysis, the activities to be secured, and the protection requirements assessed on the basis thereof. In this regards, the NED contains provisions regarding the definition of the DBT. The aforementioned regulation also provides the basis for the concept of security zones as defined in its text, and section 6 of the regulation specifies *inter alia* that operators have to demonstrate the effectiveness of their security arrangements against the threats and that this effectiveness will not be significantly reduced by any failure or malfunction of a single security system. The YVL A.11 contains many provisions which support a risk informed approach, in particular the guide mentions:

- The operator should plan nuclear security in a way that the physical protection system is able to withstand the DBT in accordance with defined protection objectives (these are currently established in the document 1/Y42217/2020 “Design basis threat for the use of nuclear energy and use of radiation” issued by STUK).
- Exercises should be conducted to demonstrate the effectiveness of the security arrangements.
- Risk analysis should be utilized in designing the nuclear facility and its structural details.
- The security assessments should be assessed regularly.
- The main functions of the organization responsible for the implementation of nuclear security should be described in the management process of the nuclear facility.
- The nuclear security design phase should be conducted logically while also taking into account the design basis and the requirements and interdependencies between the system and component designs.
- The operator’s countermeasures implemented in case of attack should be based on situational threats and risk assessments.

(Public) In a similar way, the guide YVL A.12 contains provisions which support a risk informed approach, in particular the licensee should design the information security management system to be effective in countering the DBT. Also, it is mentioned in this guide that threats and risks to information security should be analysed in a systematic manner, and protective measures should be selected on the basis of this analysis.

(Public) During its mission, the IPPAS team received many explanations from STUK on its management process, to enable them to conclude that STUK does have a risk oriented management process. However, the IPPAS team noted that numerous risk oriented provisions presented by STUK (e.g. in the documents YTV 1.a and YTV 6.c and also in the guides YVL A.3 and YVL B.1) were primarily referring to safety instead of safety and security (see title III.1.2)

VI.2 Graded Approach

(Public) In general, concerning the risks of unauthorized removal of nuclear material and sabotage, the IPPAS team, based on the documents provided to it, and the discussions held with STUK, noted that there is not a clear graded approach based on the risk of theft, and not a clear graded approach based on the risk of sabotage. However, the IPPAS team noted that YVL A.11 specifies that the rules it contains

are applicable for class 1 facility following the classification presented in the following table. This classification can depend in very specific cases on the nuclear material the facilities may contain (indeed a nuclear power plant will always be considered as a class 1 facility even if it does not store or process nuclear material of category I). For class 2 and class 3 facilities, the guide specifies that STUK can partly moderate the application of the provisions of the guide.

Facility class 1	Facility class 2	Facility class 3
nuclear power plant	research reactor	
dry or pool storage of spent nuclear fuel	processing or final disposal facility of high level nuclear waste	processing or final disposal facility of low or intermediate level waste
Category 1 nuclear material processing or storage facility	Category 2 nuclear material processing or storage facility	Category 3 nuclear material processing or storage facility

(Public) The IPPAS team noted that there is a comprehensive graded approach associated to the threat included in the legislative and regulatory framework (see titles V. and VI.1).

VI.2.1 Risk of unauthorized removal of nuclear material

(Public) Concerning the risk of unauthorized removal of nuclear material, the basis of the graded approach is set in Table 2 of the guide YVL A.11.

Material r = enrichment level (atom %)	Category 1 m = mass (kg)	Category 2 m = mass (kg) A = activity (Bq)	Category 3 m = mass (kg) A = activity (Bq)	Source material
Plutonium-239	$m \geq 2$	$0,5 < m < 2$	$0,015 < m \leq 0,5$	natural uranium (uranium containing a mixture of the U-235 isotope occurring in nature), depleted uranium and thorium
Uranium-233	$m \geq 2$	$0,5 < m < 2$	$0,015 < m \leq 0,5$	
Uranium-235	$r \geq 20$	$1 < m < 5$	$0,015 < m \leq 1$	
	$10 \leq r < 20$	$m \geq 10$	$1 < m < 10$	
	$0,71 < r < 10$		$m \geq 10$	
Nuclear waste		spent nuclear fuel ¹ nuclear waste not containing nuclear material in which $A > 1 \times 10^{15}$	nuclear waste not containing nuclear material in which $1 \times 10^{12} < A \leq 1 \times 10^{15}$	

¹ Spent nuclear fuel may belong to Category 1 based on the amount of nuclear material it contains, provided that the radiation level at 1 metre's distance from the fuel does not exceed 1 Gy/h. [2021-02-12]

(Public) Table 2

(Public) The IPPAS team noted the fact that the mass thresholds that are applicable for the total mass of plutonium in the NSS No. 13, are in YVL A.11 applicable for the mass of the isotopic 239 of plutonium, which leads to a less stringent approach than the one presented in the NSS No. 13.

(Public) Basis NSS No. 13, para, 4.5: 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.”

(Public) Recommendation 3: The categorization table (currently provided in Table 2 of YVL A.11) should be amended to be consistent with the total plutonium mass thresholds provided in Table 1 of the NSS No. 13.

(Public) The IPPAS team noted that there was no link between the categories of nuclear material mentioned in Table 2 and the definitions of the security zones provided in YVL A.11 and their associated security rules. In particular, the IPPAS team noted that it is not clearly defined in which security zone (restricted area, plant area and “protected area”) the different category of nuclear material (I, II and III) must be used and located.

(Public) Basis NSS No. 13, para 3.44: “For protection against unauthorized removal, the State should regulate the categorization of nuclear material in order to ensure an appropriate relationship between the nuclear material of concern and the physical protection measures. For protection against sabotage, the State should establish its threshold(s) of unacceptable radiological consequences in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection.”

(Public) NSS No. 13, para 4.5: “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.”

(Public) Recommendation 4: The graded approach relating to the risk of unauthorized removal of nuclear material should be based on the categorization of nuclear material as provided in NSS No. 13. In particular, the security zones, the definition of which should be based on the risk of theft, should be defined based on the category of the nuclear material they might contain.

(Public) Following that, some administrative measures, security measures and provisions associated to those security zones should also be based on the categorization table.

VI.2.2 Risk of sabotage

(Public) Concerning the risk of sabotage, the IPPAS team noted that the definition of the vital area provided in YVL A.11 considers the notion of significant radiological consequences. However, the IPPAS team was informed that no High Radiological Consequence (HRC) threshold has been defined by STUK, nor by any other Finnish competent authority. Also, the IPPAS team was informed that no Unacceptable Radiological Consequence (URC) threshold has been defined above which specific security measures addressing the risk of sabotage should be applied; however, for each DBT level there is a defined threshold for radiological consequences that shall not be exceeded. While vital areas have been already identified in the past (e.g. in OL1 and OL2), it was explained by STUK that it had not defined any consistent and systematic vital area identification process methodology.

(Public)Basis NSS No. 13, para 3.44: “For protection against unauthorized removal, the State should regulate the categorization of nuclear material in order to ensure an appropriate relationship between the nuclear material of concern and the physical protection measures. For protection against sabotage, the State should establish its threshold(s) of unacceptable radiological consequences in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection.”

(Public)NSS No. 13, para 5.8: “If the potential radiological consequences of sabotage exceed the State’s unacceptable radiological consequences, then the operator should identify equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to this condition as potential sabotage targets and protect them in accordance with the following design process (paras 5.9–5.19) and protection requirements (paras 5.20–5.43). The results of safety analysis provide useful input, including target identification and potential radiological consequences, and should be considered during design of the physical protection system.”

(Public)Recommendation 5: STUK should define a consistent and systematic methodology for the conduct of the vital area identification process.

(Public)Suggestion 4: STUK should consider hosting a training course regarding the methodology to be used for the vital area identification. The content of this course could be based on NSS No. 16.

(Public)In this context, the IPPAS team considers that the relationship between the dose values provided in the document 1/Y42217/2020 “Design basis threat for the use of nuclear energy and use of radiation” issued by STUK and the URC and HRC to be defined could be established in order to reach a consistent approach. However, it should be clear that the values provided in this document and the thresholds to be defined for the vital area identification process do not fit the same purpose.

VI.3 Defence in Depth

(Public)STUK regulation Y/3/2020 mentions that different types of security zones are placed within each other so that Structures, Systems, Components (SSCs) important to safety, nuclear material and nuclear waste are protected, based on their safety significance, and access control and goods traffic can be arranged appropriately. This regulation also specifies that these security zones must have arrangements in place to enable the detection of threats. From this basis, YVL A.11 specifies the following for nuclear facilities:

- For facilities of class 1 and class 2, four different types of security areas are defined.
- The security zones should be separated appropriately.
- The plant area/site area should be located inside the restricted area. The restricted area should be an adequately large area where movements are limited. The plant area/site area consists of a double-fenced area surrounding the buildings in which the nuclear material is located and in which the important operations are performed.
- The protected area is an area delineated by the outer wall of the aforementioned buildings. This area must be located within the plant area/site area.
- The vital area should be completely located inside the protected area.
- Specific security rules and measures apply to these areas depending on their type.

- The interfaces of security zones should form obstacles that are balanced and sufficiently effective to prevent or delay unauthorised access in order to provide the security organisation and police authorities with sufficient time to respond.

(Public) The IPPAS team did not find in the regulation Y/3/2020 and YVL A.11 any specific provisions relating to the interface between the NMAC and nuclear security. However, the IPPAS team noted YVL D.1 contains such provisions and also provisions relating to the interface between safeguards and security. In particular, this guide mentions the following:

- While considering the control methods employed by STUK, the European Commission and the IAEA, operators should plan the use of the nuclear facility taking into consideration the nuclear security arrangements so that the security regime is not compromised.
- For the nuclear facilities, the operators should ensure that the person in charge of safeguards activities collaborates with the person in charge of the nuclear security arrangements.
- For the places where nuclear material is used but which are not part of nuclear facilities, the operators should describe their nuclear security arrangements in an annex of the nuclear safeguards manual.
- All operators, including when they do not operate a nuclear facility, should store nuclear material in places where unauthorized access is effectively prevented. The operators should designate a person responsible for ensuring that nuclear material is only stored in such places. The operators should ensure that the responsible person has the necessary authority to perform their mission.
- In case of temporary transfer of nuclear material outside of its storage place, the abovementioned person should assume the responsibility for this transfer and should acknowledge the receipt when the material is brought back to its storage place. In addition to that, the transfer should be approved by the person in charge of safeguards who should be informed about the person who will arrange the transfer.

(Public) Based on the aforementioned points and the current status of the nuclear industry in Finland, the IPPAS team considered that there is a satisfactory basis for managing the NMAC as a strong mean to reinforce and sustain the security, in particular against the insider threat.

VII. SUSTAINING THE PHYSICAL PROTECTION REGIME

VII.1 Security Culture

(Public) The IPPAS team was told that the principal approach in Finland is that safety culture covers all domains: safety, security, and safeguards. A separated “security culture” is not used, instead the term “organisational culture” would be preferable, but this is not yet routinely used in the STUK guidelines. In the Finnish language there is no clear distinction between safety and “security”. YVL A.11 para 408 says that the term “safety culture” covers “security culture” and that “when designing, constructing, operating and decommissioning a nuclear facility, a good safety culture shall be maintained.”

(Public) For enhancing its own safety culture, STUK ensures senior management commitment to several activities such as establishing safety and quality policy. STUK has several cultural development programmes including assessment programmes, reporting systems and personnel training. The IPPAS team was also informed that several actions have been taken to strengthen the safety culture at STUK. One is the independent safety culture assessment which is conducted by external experts. Another example is the Country Specific Safety Culture Forum which is a joint project by Nuclear Energy Association, World Association of Nuclear Operators (WANO) and STUK to assess national culture in Finland. STUK has utilized these external assessments to establish a systematic safety culture development programme.

(Public) The IPPAS team was informed that STUK has been making efforts to enhance the importance of its organisational culture.

(Public) The IPPAS team was informed that in the abovementioned joint project by Nuclear Energy Association, WANO and STUK, it was concluded that in Finnish culture, trust plays an important role. Finns commonly have an assumption that other Finns are trustworthy. Trust of the Finns may also be abused, leading to situations where trust can be taken advantage of.

(Public) The IPPAS team has concerns on the fact that Finnish cultural traits regarding trust can prove to be a vulnerability against nuclear security threats, in particular, but not limited to the insider threat. In that context, having only one word covering safety and security, without sufficient explicit statements on security specificities could be insufficient. This could be particularly relevant for computer security, where passive and unwilling insider threat (like phishing technique for example) are a significant concern.

(Public) **Basis** NSS No. 20, 3.12: “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: (c) Developing, fostering and maintaining a robust nuclear security culture.”

(Public) NSS No. 13, 3.50: “The State should promote a nuclear security culture and encourage all security organizations to establish and maintain one. A nuclear security culture should be pervasive in all elements of the physical protection regime.”

(Public) **Recommendation** 6: STUK should give due priority and promote nuclear security culture and integrate nuclear security culture in the management system.

(Public) The IPPAS team considers that the use of the term “organisational culture”, instead of “safety culture” as the overarching umbrella which covers all elements of culture in the STUK guidelines as well as in the management system of STUK might be more appropriate to enhance nuclear security culture in Finland.

VII.2 Quality Assurance

(Public) Regulation requires the operator to have a management system. The NEA Section 7j stipulates: the management system of a nuclear facility shall pay particular attention to the impact of safety related opinions and the attitudes of the management and personnel towards the maintenance and development of safety, alongside systematic operating methods and their regular assessment and development. With respect to quality assurance, appendix D of YVL A.11 stipulates that the licensee needs to maintain a quality management programme covering all relevant fields of activity and operating areas to ensure nuclear security.

[REDACTED]

(Public) Based on international standards such as ISO9001, ISO17025 and IAEA requirements, STUK has established its integrated management system. It is assessed by means of self-assessment, independent assessments, internal and external audits and management reviews in a regular basis. The results of these assessments are recorded in a database that STUK has established and required corrective actions have been taken to improve the integrated management system.

(Public) Based on these and further observations, the IPPAS team considers the requirements and arrangements to sustain quality assurance to be sufficient.

VII.3 Confidentiality and Trustworthiness

VII.3.1 Confidentiality

(Public) With regard to confidentiality, the Act on the Openness of Government Activities provides the legal requirements for the confidentiality of official documents. The act stipulates that an official document shall be classified if it has been specified in the act or in other acts, if it has been classified by an authority on the basis of an act, or if it contains information covered by the duty of non-disclosure, as provided in an act. The IPPAS team was informed that in the nuclear energy sector, official documents can be documents drafted by STUK or other competent authorities. In specific cases, it can also be documents drafted by the operators and submitted to STUK or another competent authority. The aforementioned act also stipulates that official documents relating to or affecting the implementation of the security arrangements of persons, buildings, installations, construction and data and communications systems are classified, unless it is obvious that access to the document(s) will not compromise the security arrangements.

(Public) The IPPAS team noted that the Government Decree on Security Classification of Documents in Central Government specifies the different levels of security that should be considered for the classification and how the levels of security should be determined generically. Also, provisions on the need to apply selected security measures based on a generic graded approach is present in this decree. The IPPAS team noted from the examination of the legislative and regulatory texts provided by STUK and related discussions with STUK and SUPO that no legal or regulatory text specifies how sensitive information connected to nuclear matters should be classified and protected using a graded approach that considers the nuclear security risks. In addition, the IPPAS team was informed that as the aforementioned act and decree are not applicable for non-official sensitive documents handled by operators, they develop their own classification and protection rules. The IPPAS understood that even if the STUK would consider that a document is not classified and protected at a sufficient level according to the spirit of the aforementioned law and decree, STUK would have limited legal right to require the operator to provide a better protection level.

(Public) The IPPAS team considers that the existing approach creates significant risks of ineffective protection of nuclear sensitive information, while a prescriptive approach for nuclear security information, with clear and detailed requirements, has proven to be effective. In addition, The IPPAS team is of the opinion that the classification and security requirements for nuclear sensitive information should be based on a graded approach that considers specifically the nuclear security risks.

(Public) Basis NSS No. 23-G, para 3.4: “The State’s relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities. These are usually based on, and in accordance with, any national security policy and requirements issued by the national security

[REDACTED]

authorities, but taking into account the special nature of the activities that involve such materials. The competent authorities should also maintain close liaison with the national security authorities in order for the national threat assessment or design basis threat to be devised (...)"

(Public) Suggestion 5: STUK should consider developing a classification and protection scheme specifically for nuclear sensitive information applicable to operators, including for "unofficial documents", in order to have one overarching system applicable to all relevant organisations.

(Public) While there are no classification rules applicable for unofficial documents, the NEA sets a basis for the protection of nuclear sensitive information as nuclear information that is in written or under other tangible form and that is not generally available, cannot be disclosed in accordance with section 78 of this act. It is specifically mentioned in this section that the obligation of non-disclosure also concerns plans relating to security. In the regulation Y/3/2020, it is mentioned that information security should be monitored with appropriate procedures to detect, prevent and analyse abnormal events and to control their consequences. This regulation also specifies that proportionate systematic procedures should be in place for the detection and prevention of unauthorized removal of confidential information.

(Public) Most of the provisions relating to information security management are present within the YVL A.12 guide. This guide is applicable for all stages of a nuclear facility and it stipulates that information security, which covers integrity, availability and confidentiality of the information, is part of the licensee's management system and security arrangements. While the title of the YVL A.12 is referring to nuclear facilities, it is mentioned in the text that it should also be considered for other organizations that have an impact on information security at nuclear facilities. The IPPAS team noted that the YVL A.12 guide comprehensively addresses the following topics: resource management, assessment, audits and the reviews of the information security management systems and the information security events management. It also presents security related rules and provisions.

VII.3.2 Trustworthiness

(Public) The IPPAS team noted that section 7i of the NEA points to, for the nuclear energy sector, section 19, subsection 1, paragraphs 1 and 4, and section 21, subsection 1, paragraph 5 of the Act on Background Checks. The IPPAS team understood from that, that persons working in the nuclear field shall be subject to background checks as they may:

- regularly process government documents that may or should be classified as security levels I or II;
- process government documents that may or should be classified as security levels III or IV (Section 21.1 of the Act on Background Checks);
- perform duties that may damage the functioning of critical infrastructure or the continuation of critical production;
- be involved in the transport of nuclear material or may have access to operating nuclear facilities or those under construction, or may have access to information affecting nuclear safety.

(Public) Indeed, the NEA mentions that the license applicants shall ensure the integrity and reliability of the persons engaged in an employment relationship or engaged in a commission relationship with a security clearance or a security clearance certificate as referred to in the Act on Background Checks if a security clearance regarding the person may be carried out in accordance with the Act on Background Checks. The security clearance must be carried out before the person is granted an independent right to

[REDACTED]

access to a sensitive area or to access to sensitive information which may be used to endanger nuclear or radiation safety, or before the participation of the person in the transport of nuclear material. The licence holder shall also ensure that a corresponding security clearance regarding the personnel of the contractors and subcontractors has been carried out.

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Three levels exist: limited background check, basic background check and extended background check. The IPPAS team was informed that for some cases SUPO can contact STUK in order to have more information on which level to apply. This collaboration between STUK and SUPO was agreed during a meeting, but no official statements exist regarding this collaboration. [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED] The IPPAS team understood from this that it contributes to ensure a better application of a sound graded approach. In the event of a negative result from SUPO, the operator will decide to allow or deny access to the individual. The IPPAS team was informed by STUK that the operators systematically follow the results of the SUPO background checks.

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) **Suggestion 6:**

[REDACTED]

[REDACTED]

VII.4 Sustainability Programme

[\(Public\)](#) The IPPAS team was informed that STUK has no comprehensive sustainability programme, although a cultural development programme, the integrated management programme as well as education and training programme has been implemented, and allocation of human, financial and technical resources has been carried out on a yearly basis based on workload estimation.

[\(Public\)](#) The IPPAS team was informed that that STUK has been facing issues recruiting experienced and skilled human resource for the preparation of transition and/or retirements of personnel. Back in 2002, Finnish organisations in nuclear field evaluated human resource situation and established an organising committee in which STUK was involved to develop and organise basic post-graduate

[REDACTED]

[REDACTED]

professional training course on nuclear safety. The first six-week training course was delivered in September 2003 and so far 18 training courses have been organised in total and more than 1,300 nuclear sector employees have attended them. Nevertheless, it is still difficult for STUK to recruit experienced and/or skilled persons in a continuous manner, especially in the domain of nuclear security and information security.

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

VIII.1 Contingency Planning at the National Level

(Restricted: [Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)](#))

[REDACTED]

(Public) The IPPAS team was also informed that there are response plans at lower levels and that joint training and exercises are conducted to ensure these sub-ordinate plans are satisfactory.

(Public) Through the relevant national legislation, the Finnish Police has been assigned with responsibilities to respond to the nuclear security events and protect the critical infrastructure, by implementing a graded approach based on the significance of the event. The national response plan is documented in the order of the National Police Board. The same order also provides clear requirements to the police departments for response to security events at the local or regional level.

(Public) Regarding the provision of resources across departments and agencies, if additional resources are required in certain local areas, a formal request is made up the individual department's or agency's chain of command and requests are prioritised at the national level by respective headquarters. So while Finland does not have a named 'contingency plan' there are adequate formal arrangements at the state level to effectively respond to emerging and actual crises.

VIII.2 Emergency and Contingency Planning Interface

(Public) There is a formal state framework for the emergency and contingency arrangements, including interfaces between the key stakeholders. The IPPAS team were informed that there are arrangements in place at the higher / state level in addition to departmental bilateral agreements and protocols for mutual support. The IPPAS team was informed by a number of the presenters that the current system for contingency and emergency planning is effective.

[REDACTED]

NUCLEAR FACILITY REVIEW (MODULE 2)

IX. OLKILUOTO 3 NUCLEAR POWER PLANT (NPP)

(Public) During this mission, the IPPAS team, accompanied by STUK inspectors, visited the Olkiluoto 3 (OL3) NPP that is operated by TVO. As part of this visit, the IPPAS team reviewed the implementation of nuclear security measures at the site.

(Public) Olkiluoto 1 (OL1), Olkiluoto 2 (OL2) and OL3 reactors are located in the Olkiluoto island (figure 8) situated in the south-west coast of Finland, at the south of the city of Pori. While OL1 and OL2 are two Boiled Water Reactor (880 MWe each), OL3 (figure 9) is a European Pressured Reactor (EPR) (1600 MWe) built by the French group Areva. The OL3 reactor technology is mostly conventional compared to other Pressured Water Reactor, but it includes several fundamental novel features, e.g.:

- Improved defense-in-depth
- Improved physical separation
- Severe accident defined as design basis

(Public) The construction of OL3 began in 2004 after the construction license was issued by the Finnish government. The reactor achieved criticality for the first time in December 2021 and its first connexion to the grid happened in March 2022. At the time of the IPPAS mission, it was mentioned that regular electric production should start in July 2022. The full handover of the facility should occur very soon between Areva and TVO.



(Public) Fig. 8: Olkiluoto island



(Public) Fig. 9: Olkiluoto 3

IX.1 Security Management Programme

IX.1.1 Threat and Target Identification

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

| [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

| [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

| [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

IX.1.2 Security Plan including Contingency Plan

(Public) The local facility security and contingency plans were not fully reviewed during the IPPAS mission but aspects of the security regime and contingency arrangements were sampled. During the site visit, a number of briefings were provided to the IPPAS team by staff from other security and emergency agencies. These briefings were complemented by demonstrations of the capabilities of these agencies. The IPPAS team was informed by the operator that all of the site security arrangements were documented in the site's security plan and in the suite of sub-ordinate general security instructions, which provide more details on the specific arrangements. The IPPAS team were talked through the security plan (written in Finnish) and some of the supporting security instructions. These seemed satisfactory, with a clear link through the hierarchy of documents.

(Public) The IPPAS team was informed that the security plan was approved by STUK, as part of the licensing process, and that these processes were also reviewed.

(Public) STUK use the term response plan to describe the contingency arrangements. Similar to the security plan, there is an overarching site response plan which broadly covers the response arrangements. This is supported by a suite of sub-ordinate documents, providing more details of the roles and responsibilities of the key response stakeholders.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

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

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

IX.1.4 Security Organization

(Public) The operator presented the organization for nuclear security at OL3.

[REDACTED]

Most operational tasks regarding nuclear security (access control, NSOs, armed response, Central Alarm Station (CAS) operation...) are provided by a subcontractor named Securitas. Securitas personnel was present during all the visit.

(Public) The IPPAS team had several opportunities to discuss with representatives from the operator and with NSOs. Explanations provided were consistent with regulations, as previously presented by STUK and other competent authorities, for example regarding:

— (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

— (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

— (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

— (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

IX.1.5 Security Staff Training and Qualification

(Public) The IPPAS team was informed that TVO maintains necessary arrangements to ensure adequate recruitment, training and qualification of security staff.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Confidential Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Suggestion 7:**

[REDACTED]

IX.1.6 Security Culture

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Suggestion 8:**

[REDACTED]

[REDACTED]

IX.1.7 Security Procedures

(Public) YVL A.11 para 316 states: The licensee shall describe security arrangements in a security plan, nuclear facility security standing order, transport security plan and other documents related to security arrangements, which shall be kept up-to-date.

(Public) The IPPAS team reviewed TVO security plan and observed that it referenced relevant nuclear security procedures.

(Restricted: [Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)](#)) The IPPAS team reviewed some of them, including:

(Public) The IPPAS team considers that TVO has implemented procedures to ensure that security matters are addressed according to the nuclear security plan and security standing order

IX.1.8 Confidentiality and Trustworthiness

(Public) The IPPAS team was informed that the operator has information security management policy and the related lower-level documents to classify and handle the sensitivity levels of “secret” and “confidential” information. The Olkiluoto NPP provides a training related to confidentiality to the entire personnel as part of the induction training.

(Public) The operator explained that security clearances are performed on all persons working at the Olkiluoto NPP based on its personnel manual, information management manual and security arrangements manual. TVO staff and security personnel takes “basic background check”, whereas subcontractors who “is involved in the transport of nuclear material or has access to a nuclear facility or access to a nuclear facility construction site or obtains information on factors affecting the safety of a nuclear facility” (Section 21, paragraph 5 of the Act on Background Checks (726/2014)) takes “limited background check”.

(Public) These security clearances are conducted by SUPO. In addition, the operator has an internal programme for detecting early warning signs and for training supervisors for this purpose. The IPPAS team was also explained that the medical personnel has a right to inform TVO on the mental health issues of shift personnel and security personnel and random drug and alcohol checks have been conducted on all persons working at the NPP.

(Public) Refer to trustworthiness chapter X regarding the graded approach for background checks.

IX.1.9 Reporting of Nuclear Security Events

(Restricted: [Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)](#))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

[REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) The Olkiluoto NPP has implemented a quality assurance programme for its physical protection system as guided by YVL A.11, para 313 “In the design, implementation and manufacturing of security-related systems, structures and components, relevant standards and quality management in accordance with them shall be followed to ensure their reliability”.

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

- (Public) all technical documentation undergoes a review-approval cycle before implementation,

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

IX.1.12 Sustainability Programme

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IX.2 Physical Protection System (PPS)

IX.2.1 Graded Protection and Defence in Depth

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Security areas following NSS No. 13	Security zones following YVL A.11
Limited Access Area	Restricted Area
Protected Area	Plant Area
	"Protected Area"
Vital Area	Vital Area

(Public) Table 3.

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

IX.2.2 Detection

[\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) **Good Practice 5:**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Recommendation 8: [REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Suggestion 9:**

(7) (Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

Recommendation 9: [REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)
Recommendation 10:- [REDACTED]
 [REDACTED]
 [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))
Recommendation 11: [REDACTED]

IX.2.4 Central Alarm Station

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Suggestion**
10: [REDACTED]

[REDACTED]

[REDACTED]

Further observation of the IPPAS team were:

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IX.2.5 Delay

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Fig. 10:

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Fig. 11:

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Recommendation

[REDACTED]

[REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

```
11: [REDACTED]
```

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

X. NATIONAL LEVEL REVIEW OF SECURITY OF RADIOACTIVE MATERIAL

X.1 Assignment of Nuclear Security Responsibilities

X.1.1 State

(Public) All information provided in the chapters II.1., II.2. and II.3. of this report regarding the legislative, executive and judicial process that was connected to the regulation of the physical protection of the nuclear materials and nuclear facilities are also applicable for the regulation of security of radioactive material, associated facilities and associated activities. Therefore, the chapters dealing with the division of the powers, general information on functioning of the government of Finland etc. will not be repeated at this place and only distinctions applicable for the security of radioactive material, associated facilities and associated activities are mentioned below.

(Public) State has the responsibility to develop an effective national regulatory system of control over the management and protection of radioactive sources and ensure that appropriate facilities and services for radiation protection, safety and security are available to, and used by, the persons who are authorized to manage radioactive sources. In order to better fulfil this commitment Finland completely revised Radiation Act, implementing decrees and issued seven completely new STUK regulations which entered into force on 15th of December 2018. The law and decrees were revised under the leadership of the MSAH in close co-operation with STUK. The reform was based on the EURATOM so-called BSS directive and was carried out in order to ensure the future safety of the continuously evolving and expanding use of radiation as well as modernize and improve regulatory activities and apply a more risk-based approach.

(Public) In addition to the abovementioned international treaties Finland expressed its political commitment with regard to the CoC including the Supplementary Guidance on the Import and Export of Radioactive Sources and Supplementary Guidance on the Management of Disused Radioactive Sources and nominated a point of contact for the purpose of facilitating the export and/or import of radioactive sources (STUK). See also chapter X.9 Import and Export of Radioactive Sources.

X.1.2 Regulatory body

(Public) STUK is the regulatory (competent) authority which falls under the jurisdiction of the MSAH (see figure 12). MAEA has supreme authority in supervising compliance with the Radiation Act in matters concerning the use of nuclear energy as referred to in the NEA.

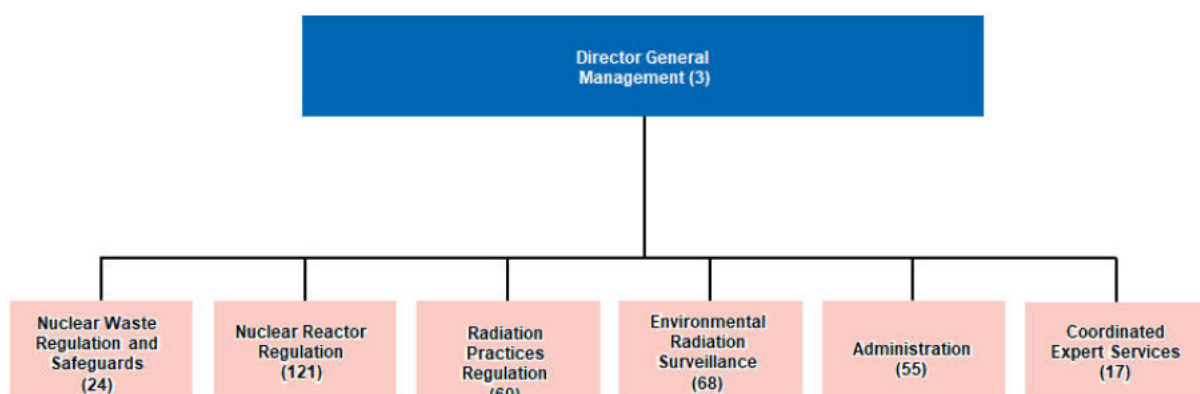


(Public) Fig. 12: STUK and Ministries

(Public) STUK was originally founded in 1958 and since that time gained more responsibilities. STUK is currently divided into 5 main departments (see figure 13):

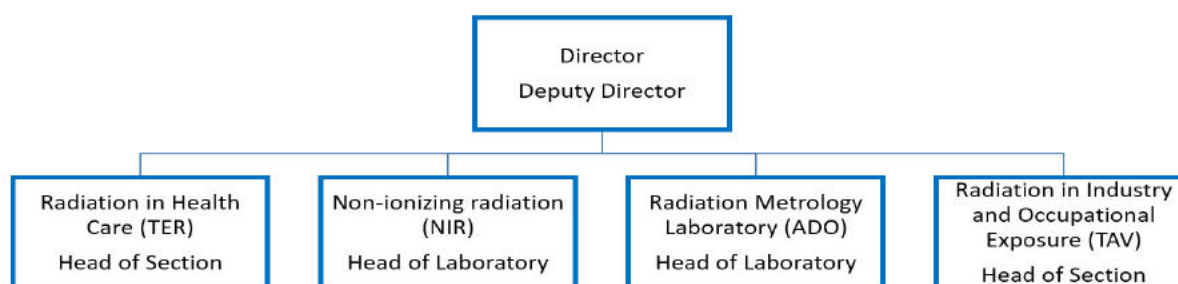
- Nuclear Reactor Regulation (YTO),
- Nuclear material and waste supervision (YMO),
- Environmental radiation surveillance (VALO),
- Radiation practices regulation (STO),
- Administration (HAL),
- Recently STUK has also established a new department – Coordinated Expert Services (APA), which cooperates with all the departments of STUK regarding the preparedness, communications, public relations and international cooperation and management and development.

(Public) STUK has currently around 330 employees. STUK has just recently moved its headquarters into the modern building in the city of Vantaa.



(Public) Fig. 13: STUK – organizational structure

(Public) STUK supervises both safety and security of radioactive sources. The Department of Radiation Practices Regulation (STO) of the STUK functions as a regulatory authority on the use of ionizing and non-ionizing radiation, conducts research in support of regulatory control and maintains metrological standards for ionizing radiation (see figure 14). STO covers both safety and security of radioactive sources. The IPPAS team was informed that the same inspectors perform safety and security inspections and each inspector in STO has basic knowledge to perform security inspection in their field of use of radiation. There is also one dedicated inspector within STO with responsibility of security matters. In case of lack of knowledge of STO, the YTS assists whenever there is any need in security matters, including training of inspectors in nuclear security. Within STUK, STO's Department of Radiation in Industry and Occupational Exposure Section (TAV) is responsible for supervising the transport of radioactive material and the basis for this supervision is given by the Radiation Act and Act on Transportation of Dangerous Goods.



(Public) Fig. 14: STO – organizational structure

(Public) STUK issues, maintains and develops nuclear security requirements in the form of binding regulation, regulatory guides and DBT. STUK is entitled to conduct inspections, investigation and to require information (section 176 of the Radiation Act) as well as to impose enforcement and coercive actions (section 177, 184 of the Radiation Act, Administrative Procedure Act). Even though that there is no specific explicit provisions on independence of STUK the IPPAS team considers that for the following reasons STUK is well established and independent regulatory authority.

- STUK is defined and its powers are enumerated by the Act (Act on Finnish Radiation and Nuclear Safety Authority, Radiation Act) and impartiality and independence of decision-making is secured through the general provisions (Administrative Procedure Act),
- STUK possess efficient and effective supervisory powers (e.g. if use of radioactive sources isn't safe or secure, the activities may be suspended by STUK, STUK conducts independent assessment of safety and security prior the authorization of activity, STUK performs independent inspections, may assess required information, impose administrative coercive measures...), and
- STUK have a budget for its regulatory activities which is partially covered by the charges payable to the State (according to the Act on Criteria for Charges Payable to the State, 150/1992 and section 192 of the Radiation Act).

(Public) STUK maintains registers under the Radiation Act - section 19. STUK grants safety licenses upon application until further notice or, for a special reason, for a fixed period of time. The license may also be granted separately for different stages of the practice. STUK issues according to the section 67

[REDACTED]

of the Radiation Act more detailed regulations on the security arrangements and their determination in accordance with the radiation sources. There is no explicit provision regarding the competence for issuing the guides in the radiation safety sector in the Radiation Act.

X.1.3 Other Competent Authorities

(Public) The MSAH has supreme authority in supervising compliance with the Radiation Act. The MEAE has supreme authority in supervising compliance with the Radiation Act in matters concerning the use of nuclear energy as referred to in the NEA.

(Public) Finnish Customs supervises, for its part, the import and export of radiation sources and radioactive waste and the consumer goods referred to in section 69 of Radiation Act as well as the transit of radioactive waste through the territory of Finland. The Advisory Committee on Radiation Safety which is appointed by the Government, operates in connection with STUK, participating in the preparation of matters related to radiation safety.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public) STUK has the regulatory oversight for the transport of Class 7 materials. TRAFICOM also participates in joint inspections with STUK and cooperates with STUK when the transport of radioactive material is arranged.

X.1.4 Operator, Shipper and/or Carrier

(Public) Responsibility of physical protection of radiation sources (Radiation sources can be X-ray equipment or radioactive substances or devices that contain them) that are used for industrial or medical purposes lies within the license holder. License is issued by the STUK. Currently there are approximately 3000 STUK licenses. This includes all practices concerning radiation sources: trade in radiation sources, manufacturing, possession, servicing, repairs, import and export of radiation sources. The IPPAS team was informed that approximately 1% from these license holders are handling with High Activity Sealed Source (HASS).

(Public) According to the section 54 of the Radiation Act license holder is obliged to furnish a security for the costs arising from rendering radioactive waste harmless and any possible environmental cleaning measures and the practice may not be commenced before the security has been furnished. The State, a municipality or a joint municipal authority is not required to furnish a security.

(Public) According to the section 67 of the Radiation Act license holders should implement security arrangements which should be adequate in terms of the risks related to the practice and the radiation sources and they must form a whole compatible with the measures concerning radiation safety. For radiation safety and security deviations operator must have a separate preparedness plan, including instructions what and how to report to the authorities.

(Public) The radiation act sets requirement for responsible party of transportation of HASS to have a safety license. Section 49 on Practices exempt from a safety license the transport of radioactive substances, excluding the road or rail transport of HASS.

[REDACTED]

(Public) Radioactive substances may only be consigned for transport by an appropriately identified carrier. Regulations on the recognition of the carrier and other provisions connected to the transport of radioactive substances are set forth in the Act on the Transport of Dangerous Goods (719/1994) and security arrangements according to the TRAFICOM regulation needs to be applied during transport. A security plan is required for the transport of high-risk radioactive material according to 1.10.3.2 of the TRAFICOM regulation.

(Public) According to these provisions the IPPAS team concludes that responsibilities for the physical protection of radiation sources of the license holders are clearly defined and allocated.

X.2 Legislative and Regulatory Framework

(Public) Finland established a comprehensive framework for the security of radioactive materials that takes into account the legislative and regulatory framework for radiation protection and safety. STUK is responsible for ensuring that proper safety and security measures are established throughout the life cycle of radioactive materials. In this context, radioactive materials includes radiation sources, radioactive substances, radioactive waste and radiation devices.

X.2.1 Laws

(Public) The Act on the Transport of Dangerous Goods (719/1994) applies to the security arrangements of transport. Additional information on the transport security legislative and regulatory framework is described in section X.10.

(Public) In Finland, the Radiation Act (859/2018) establishes the requirements for radiation practices, exposure situations and medical and occupational exposure to non-ionizing radiation (see figure 15). The MSAH has supreme authority in supervising compliance with this Act. The purpose of this Act is to protect human health against the detriments caused by exposure to radiation. The Act also aims to prevent and reduce environmental and other detriments of radiation. This law came into effect in December 2018. STUK supervises compliance with this Act.



(Public) Fig. 15: Radiation Act in the regulatory framework

(Public) According to the Act section 67: “security arrangement are proportionate to the risk related to the practice and the radiation sources”. Section 67 also contains high level security requirements for radiation sources that include provisions for security plans, structural barriers, the presence of personnel, conducting inventory verification and restricting access to the materials.

(Public) The Act requires a safety licence (authorization). As part of the licence application, applicants must demonstrate compliance with safety and security requirements. The Radiation Act stipulates that the party running a radiation practice (the licence holder) is responsible for the safety of the operations. This includes the responsibility for security. STUK is responsible to authorize, inspect and enforce safety and security requirements for radioactive materials. This includes the review and approval of security plans.

(Public) The IPPAS team noted that the Radiation Act refers to safety in several requirements without explicitly mentioning security. For example, security is not mentioned in sections 12 *safety culture and safety management*, 26 *safety assessment concerning radiation practices*, , 30 *quality assurance and section 33 training*. The IPPAS team was informed that security was considered to be included in safety requirements.

(Public) The IPPAS team also noted that:

- STUK reviews and approves security plans during the safety licensing application and before granting an authorization. SKV 3.2 guide provide instructions on how to handle application. STUK guide 9.5 provides guidance on classification and marking of documents. This covers security plans, transport security plans, inspections reports and notifications that contain sensitive information,
- the review and approval of security plans for radioactive sources level A and B is under the responsibility of the STO inspector who handles it. STO may request support from YTS to assess the security plan, and

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

- STO is in the process of developing an internal annexe to the inspection guide to provide instructions on the supervision of security arrangements for radioactive sources. This will include a checklist for the security inspections.

(Public) The IPPAS team observed that there is no process or guide for STO personnel in TER and TAV to ensure security plans are appropriately reviewed and assessed in a consistent manner with the support of YTS.

(Public) **Basis** NSS No. 11-G, para 3.3: “The regulatory body’s assessment of each application for an authorization should...ensure...that the final security measures are verified to be acceptable in accordance with established criteria and procedures.”

(Public) **Suggestion 12:** STUK should develop an internal process to ensure the timely and consistent review of security plans. This process should be tied to the authorization and licensing process and should include the protection of sensitive information (e.g. security plan, security inspection reports and deficiencies).

(Public) The IPPAS team encourages STUK to take into considerations the findings from the IPPAS mission and prioritise the development and implementation of the annexe for security inspections.

X.2.2 Regulations

(Public) In 2018, STUK published regulation (S/3/2018) on the security arrangements of radiation sources. This regulation was revised in 2021 (S/9/2021) to include minor changes. The regulation applies to sealed radioactive sources, unsealed sources and mobile X-ray equipment. This includes radioactive substances, radioactive waste and radiation devices.

(Public) This regulation established three security levels A, B and C based on the activity of the radionuclide, its form and quantities. The appendix contains a list of radionuclides with the activity thresholds. The regulations sets specific security requirements for each security level based on this categorization system (see table 4). The regulations also contains requirements for the content of the security arrangement plan (e.g. security plan).

Category C (IAEA categories 4 and 5)	Category B (IAEA categories 2 and 3)	Category A (IAEA category 1)
Sources above clearance level Mobile X-ray devices	(< 1000 x HASS) For example: 1. Co-60 20 GBq 2. Cs-137 100 GBq 3. Am-241 60 GBq Mobile x-ray-radiography devices	(> 1000 x HASS) For example: 4. Co-60 20 TBq 5. Cs-137 100 TBq 6. Am-241 60 TBq
Requirements: 7. One structural barrier 8. Access only to persons tasked with taking care of the place of use or storage	Requirements: 9. Category C requirements 10. Two structural barriers. <i>The structural barriers may be replaced by having personnel on site.</i> 11. Access only to persons tasked with taking care of the place of use or storage 12. Security plan 13. Access control 14. Alarm system 15. Sources must be verified monthly, verification must be documented 16. Sensitive information must be protected	Requirements: 17. Category B and C requirements 18. Two structural barriers. <i>The structural barriers may not be replaced by having personnel on site.</i> 19. Surveillance cameras 20. Security plan must be revised every three years

(Public) Table 4: Security levels A, B and C established by STUK classification for radioactive sources

(Public) STUK security guide provides additional instructions on how to meet the regulations. This guide also contains requirements and guidance for the security arrangements that must be applied in all uses of radiation subject to a safety licence.

(Public) The IPPAS team noted that in the regulation S/9/2021 and security guide:

- there are no references to the Act on Background Checks section 21 paragraph 5 that states that a limited background check (concise) may be conducted for persons that handle and transport

HASS. [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

- there are no designations or classifications for the protection of sensitive information. Only the security plan must be kept in a secure manner and available for those that need to know as part of their duties. The IPPAS team was told that security plans are submitted to STUK by regular emails. Once they are received, they are classified by STUK and labelled restricted,
- there are no security requirements for security training or qualifications for personnel who handle, use and transport radioactive materials,
- there are no requirements for alarm testing or performance testing verification to verify the effectiveness of security measures for level A and B,
- there are no requirements for alarm response arrangements with onsite and off-site response forces for levels A and B,
- the STUK requirement to conduct verification of the radioactive source is monthly for security level B. The NSS No. 11-G guidance section 6.14 suggest weekly verifications for level B,
- the security guide document uses ambiguous verbs that makes it difficult to differentiate between “must”, “can”, “may” or “should”. Some of the performance based objectives may be misinterpreted. In some cases, there are no compliance criteria that can be enforced by STUK inspectors, and
- the requirements for the content of the security plan are not fully aligned with NSS No. 11-G guidance.

(Public) The IPPAS team noted that the requirements for some security measures are unclear, inconsistent and sometimes ambiguous. There is no specific guide for security inspections for radioactive sources. As a result, the inspectors need to interpret security requirements which could result in inconsistencies in the application, verification and enforcement of the regulations.

(Public) Basis NSS No.14, para 3.8: “The State should establish requirements in accordance with national practices to ensure appropriate protection of specific or detailed information, which could compromise the security of radioactive material, associated facilities and associated activities if the information were disclosed”.

(Public) NSS No.14, para 4.13: “Response measures should be implemented following detection and assessment. The *operator* should be required to make appropriate arrangements to communicate with law enforcement personnel following detection and assessment in order that they may perform the response. In implementing a *graded approach*, the objectives of response measures could range from providing immediate response with sufficient resources to interrupt *malicious acts* to providing alarm notification to allow the appropriate authority to investigate the event.”

(Public) NSS No.14, para 4.16: “*Operators* should be required to implement security management measures, addressing access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory and event reporting. The stringency of required security management measures should vary as appropriate based on the *graded approach*.”

(Public) Recommendation 13: STUK should clarify and revise the security requirements that are set out in the security guide and in the regulation S/9/2021 to include new security requirements for information security, trustworthiness, security awareness training, frequency of verification and response arrangements to align with NSS No. 14.

(Public) Suggestion 13: STUK should consider adding and also revising requirements for the maintenance and testing of security measures and update the content of the security plan based on NSS No. 11-G.

X.2.3 Trustworthiness verification

(Public) To address the previous IPPAS Recommendation R28 (2012): “*Formal trustworthiness checks should be a requirement for individuals with access to radioactive sources to help counter any potential insider threat. The level of trustworthiness required should be detailed in the legislation*”. STUK submitted a proposed amendment for the Act on Background Checks. The revised Act section 21 paragraph 5 states that a limited background check (concise level) may be conducted for:

“(5) is involved in the transport of nuclear material or has access to a nuclear facility or access to a nuclear facility construction site or obtains information on factors affecting the safety of a nuclear facility or access to a nuclear material storage facility or to a site or storage facility with a level of radioactive material equal to or greater than the level of high activity sealed radioactive material within the meaning of radiation legislation”

(Public) This Act allows for trustworthiness checks for persons with access to HASS and sensitive information.

(Public) During the IPPAS mission, the IPPAS team noted that:

- STUK regulations S/9/2021 does not require mandatory trustworthiness verifications and background checks for security levels A and B. This is only a recommended practice stated in the security guide;

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Suggestion

X.2.4 National Registry and Inventory of Radioactive Sources

(Public) STUK requires licenses to maintain their own registers. STUK regulation S/9/2021 also requires operators with levels A, B or C to verify radiation sources in their possession monthly and to maintain documents of these verifications. At the time of the IPPAS mission, there were approximately 3000 safety licenses delivered by STUK. This covered the industrial, research, veterinary and healthcare sectors (see table 5).

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) Section 19 of the Radiation Act gives the responsibility for STUK to maintain a national registry for radioactive sources above exemption level. STUK established and maintains a centralised database VASARA with registers of radioactive sources and radiation devices. VASARA includes information on safety licence, licence applications, radioactive sources, occupational dose and other information related to the safety of the facilities and its activities. VASARA includes category 1 to 5 sources, unsealed source and any other practices that requires a safety licence by STUK. It is also used for the planning of inspections. SAHA is used for tracking deviations (non-compliance) issues.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) STUK maintains a centralized information management system VASARA that contains all registers of safety licences. This system includes licensing, compliance, event reporting related to the safety and

security of radioactive sources. Information security is integrated in VASARA to protect sensitive information and to restrict access to personnel with the need to know as part of their duties.

X.3 International Cooperation and Assistance

(Public) The IPPAS team was informed that STUK is a point of contact for Finland in international exchange systems maintained by the IAEA and the European Union to report issues related to radioactive sources. Representative of STUK STO is the point of contact for IAEA's Incident and Trafficking Database (ITDB). Finland is a member of ITDB since 1995. The representative of STUK STO participates to the IAEA's Working Group on Radioactive Material Security, IAEA training courses and other meetings regarding the security of radioactive sources.

(Public) Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency was approved by the State in 1986.

(Public) Finland made its political commitment with regard to the CoC, also notified IAEA of its intention to act in accordance with the two supplementary guidance. See more in chapter X.9.

(Public) Overall the IPPAS team noted that STUK is on its way to fully implementing the security provisions of the IAEA CoC.

X.4 Identification and Assessment of Threats

(Public) A DBT was established for radioactive sources and small quantities of nuclear materials. STUK maintains the DBT. STUK has updated the DBT for the use of radiation and considered the DBT as a basis for the requirements and guidance related to the security of radioactive sources. Radioactive material, radiation devices and small quantities of nuclear material outside nuclear facilities have one set of adversary characteristics in the DBT, and the protection objectives vary progressively by material category, which reflects the potential consequences. The protection objectives based on the DBT could be found in figure 16.

Class of nuclear or other radioactive material	A	B		C	
	IAEA cat 1 radioactive material	IAEA cat 2 and 3 radioactive material, industrial radiography equipment	NM outside NF, extensive use	Other radioactive material, mobile x-ray equipment	Other NM outside NF, other nuclear items (technology dual use, information)
Threat	Protection objective				
Intentional, unlawful activity, e.g. sabotage, theft	Prevent/stop	Minimize risk	Minimize risk	Reduce risk	Reduce risk
Loss, unauthorized handover	Prevent/stop	Minimize risk	Minimize risk	Reduce risk	Reduce risk
Proliferation			Prevent/stop		Prevent/stop

(Public) Fig. 16: Protection objectives for the security of radiation sources.

(Public) In line with 1/Y42217/2020 the material specific DBT for radiation sources is in Appendix F which is classified (Confidential SC III).

(Public) The STUK regulation S/9/2021 contains the requirements of the security arrangements for each security level (A,B,C). Finland has 3 security levels for radioactive sources. Security requirements are derived from the DBT, graded according to the security level of the source. See more about categorization in X.2.2.

(Public) The IPPAS team observed that devices generating ionizing radiation without containing radioactive sources are also covered in the protection objectives and subject to security levels.

(Public) Overall, the IPPAS team found that STUK has established and maintains a DBT for radioactive sources and small quantities of nuclear material in alignment with the recommendations from the CoC and NSS No.14.

X.5 Risk Based Nuclear Security Systems and Measures

X.5.1 Risk Management

(Public) In accordance with Section 67 of Radiation Act 859/2018: “security arrangements shall be adequate in terms of the risks related to the practice and the radioactive sources”. Security requirements for radioactive sources are also based on a risk-informed approach. Based on the guidance on the security arrangements issued for the STUK regulation S/9/2021 the security plan includes risk management. The protection measures have to be proportionate with the identified risks. The organisation maintains a description of the security arrangements and the conclusion of the risk management process has been taken into account in the organisation’s security documentation. The plan also should contain a chapter about assessing security and the assessment could support risk management as well.

(Public) The inspection programmes are risk-informed. For radioactive sources, the security levels are considered when planning and executing the inspection programme in terms of inspection depth and frequencies. On a risk-informed approach, the experts from YTS could participate in these inspections as consultants with STO representatives.

X.5.2 Interface with the Safety System

(Public) The IPPAS team was informed that STUK is a “3S-house”. The IPPAS team noted that the relationship between YTS and STO is robust. They can conduct joint inspections and participate in safety-security exercises. The Radiation Act 859/2018 also contains references to both safety and security. In accordance with the provisions of Section 51 of Radiation Act the application for safety license shall include inter alia both the safety assessment concerning the radiation practice (Section 26) and the plan on the security arrangements (Section 67). In accordance with Section 67 of the Radiation Act 859/2018, security arrangements must be compatible with the measures concerning radiation safety. See more in chapter X.2.

(Public) Based on the guidance issued for the STUK regulation S/9/2021 on the security arrangements of radioactive sources that requires a safety license, the security plan includes safety (security) culture, and procedures for safety and security related communication.

(Public) The IPPAS team was informed that all the inspectors in STO who are dealing with safety licenses received basic security training. There is one STO inspector who is dedicated to the security of radioactive sources, and in case of a question or doubt the other inspectors can easily request assistance from that inspector. Additionally YTS upon request by STO, serves as an expert when assessing the

[REDACTED]

security arrangements of HASS. STUK also regularly conducts joint inspections for safety and security. There is an internal working group which includes participants from all Departments of STUK. This internal working group meets 3-4 times a year and minutes of these meetings are documented and tracked within the management system. One of the objectives of this working group is also to share knowledge about safety and security.

(Public) The IPPAS team was informed that STUK uses HAKE to record all the observations (both negative and positive) taken by the inspectors during inspections. Deficiencies (non-compliance or findings) that contain sensitive information is restricted. This system covers both safety and security observations and the system is available for all STUK inspectors that have the need to know to perform their duties. On a monthly basis the findings are discussed between the representatives of the departments. This tool could also be used to identify trends, for example security culture.

(Public) The IPPAS team noted that HAKE is a very useful tool to track corrective actions. However, STO does not use HAKE. The IPPAS team encourages STO to use HAKE to share operational experience and information for security inspections findings and lesson learned with other inspectors. This would assist STUK in enhancing information sharing between those responsible for safety and security.

(Public) Basis NSS No. 11-G, para 3.102: “There should be regular, systematic cooperation and information sharing between personnel in the regulatory body responsible for the development and implementation of safety requirements and those responsible for the development and implementation of security requirements. This cooperation and information sharing could include, but is not limited to...Shared inspections, as much as the protection of information allows for them...”.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Suggestion 15: [REDACTED]

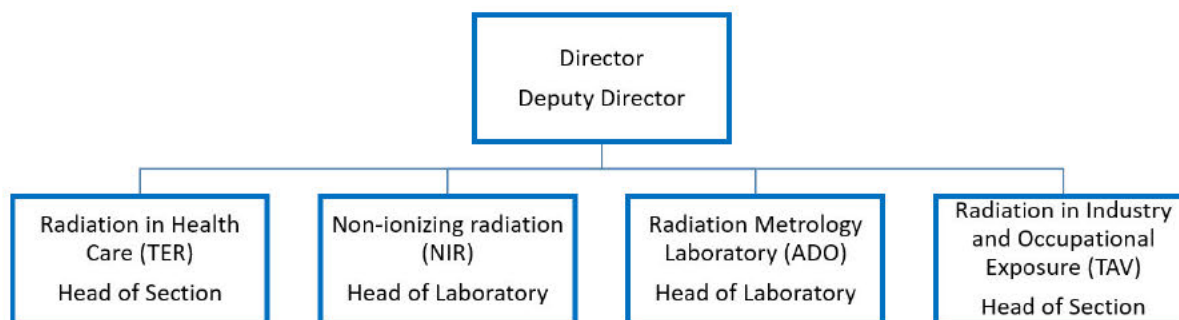
(Public) Overall, the IPPAS team observed that there are several interfaces and coordination mechanisms established between YTS and STO that are mutually beneficial.

X.6 Sustaining the Nuclear Security Regime

(Public) Under the current legislative and regulatory framework, STUK STO receives a budget from MSAH for the oversight of safety and security of radioactive sources. This includes human and financial resources to supervise activities associated with licensing, compliance and enforcement.

(Public) There are two sections (TER and TAV) in STO that are responsible for conducting safety and security inspections of radioactive materials in the medical and industrial sectors (see figure 17).

[REDACTED]



(Public) Fig. 17: STO organization structure

(Public) The IPPAS team was told that:

- There is one trained and qualified inspector in TAV who conducts security inspections. There was no evidence that TER inspectors trained or qualified for security inspections.
- In the past two years (2020-2021), there were no security inspections conducted due to the COVID 19 pandemic. Before the pandemic, there were very few security inspections conducted.
- Safety inspections are prioritized over security inspections.
- Because of concurring operational projects and priorities, it is a challenge to dedicate time and resources for security inspections.

(Public) The IPPAS team noted that:

- Every inspector in STO has basic knowledge to perform security inspections in their field of expertise. However, there is no specific or mandatory training on the security of radioactive materials that follows a systematic approach to training.
- There is an internal guide YTV 3.c.5 that includes roles and responsibilities and oversight to assess the security arrangements for radioactive sources. This guide does not include the sharing of sensitive information, training and security plan assessment.
- YTS can provide support to STO for any inquiries or requests related to security of radioactive materials. STO and YTS can conduct joint inspections upon request from STO.
- There is no succession plan (long term commitment) to sustain human resources. The knowledge and competence currently resides on one inspector.

(Public) **Basis** CoC, para 21: “Every State should ensure that its regulatory body: (b) has the financial resources and the facilities and equipment necessary to undertake its functions in an effective manner”.

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

(Public) **Recommendation 15:** The State should ensure that STUK has sufficient human and financial resources to:

- train inspectors on the security of radioactive materials,
- conduct security inspections for HASS use, storage and transport following a graded approach and
- develop a long term plan for human resource development.

Security culture for the security of radioactive materials

(Public) As mentioned previously, security culture is part of safety culture. STUK promotes safety culture and conducts safety culture oversight. Since the primary focus in the Radiation Act is on safety culture, operators follow the same philosophy.

(Public) The IPPAS team observed that in Finland all organizations involved in the nuclear security regime believe that the threat is real and credible. They also recognize the importance of nuclear security. YTS participate in management meetings and security is considered in all operational activities.

(Public) Overall, the IPPAS team found that the Finland maintains a comprehensive legislative and regulatory framework for the security of radioactive materials. The IPPAS team observed that nuclear safety is established and promoted. Areas for improvement include promoting a security culture among all individuals and in all bodies involved in the management of radioactive sources, developing security training and allocating adequate human resources to sustain the regulatory compliance activities for the security for radioactive materials in use, storage and transport. For additional information, refer to Chapter VII.1

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

(Public) Finland has a comprehensive national response framework for nuclear and radiological emergencies. Finland has established and maintains Chemical Biological Radiological Nuclear Explosive (CBRNE) response capabilities and a CBRNE strategy. There is also a national CBRNE coordination committee. STUK is part of that committee.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) STUK maintain a 24/7 on call system to initiate response in case of abnormal events. STUK experts support other authorities in case of a nuclear security event. During the mission, the IPPAS team visited STUK's new Emergency Operation Centre and commends STUK for their new facility.

(Public) In case of a nuclear security event, STUK can provide expertise in nuclear and radiation safety with regards to protecting the population, first responders and analyse radiation measurements in the field. STUK also participate in training and joint emergency exercises on a regular basis.

(Public) For radioactive sources, STUK recommends licenses to notify the police in case of a security event (ex: theft). The security guide provides guidance on how to prepare for a radiation safety incident and recommends licensees to document their communications in exceptional circumstances in their security plan. The security guide recommends to make arrangements with the local police department to agree on the procedure for ensuring immediate notification. The IPPAS team noted that there are no

[REDACTED]

requirements for response arrangements with the police in the Radiation Act or in the regulations S/9/2021.

(Public)Basis NSS No.11, para 3.114: “The regulatory body should require the operator to include measures in its security plan that ensure a timely and effective response to a suspected, attempted or actual malicious act involving radioactive material within the facility”.

(Public)Suggestion 16: STUK should consider including a requirement in the regulation S/9/2021 to ensure licensees with security levels A and B implement measures to ensure a timely and effective response to attempted or actual malicious acts involving HASS.

(Public)STUK provides a list of locations with the most dangerous radioactive sources to the Police on an annual basis. This information is used by the emergency center (112) to prioritise response and to give first responders relevant information that could facilitate their intervention and their own safety. The list is compiled following a security risk assessment methodology by STO. This assessment considers several criteria such as radioactive source activity, location, mobility, dispersability, attractiveness and risks.

(Public)Good Practice 7: STUK provides a list of high risk source locations to the police on an annual basis with relevant information on the material attractiveness and associated risks to support first responders safety and prioritise rapid response.

X.8 Detection and Reporting of Nuclear Security Events

(Public)For STUK reporting requirements for operators refer to response arrangements in chapter X.7

(Public)STUK has established and maintains a framework agreement with Finnish Customs to detect Material Out of Regulatory Control and unlawful activities. Customs has the authority to control the import and export of radiation sources and radioactive waste according to the Radiation Act (859/2018). Customs ensures that class 7 materials imports and exports have the appropriate safety licence approved by STUK. The IPPAS team was told that this cooperative framework between the two organisations allows them to share timely information and provide mutual support.

*(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))*Fig. 18:

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public) Overall, the IPPAS team found that Finland maintains comprehensive national capabilities to detect nuclear security events originating from radioactive materials.

X.9 Import and Export of Radioactive Sources

(Public) Finland made its political commitment to the CoC and also notified the IAEA of its intention to act in accordance with the Guidance on the Import and Export of Radioactive Sources and the Guidance on the Management of Disused Radioactive Sources. Finland nominated a point of contact for the purpose of sharing information and facilitating the export and import of radioactive sources. STUK is the point of contact.

(Public) The IPPAS team was informed that import and export of category 1 and 2 sources are carried out in accordance with the provisions of CoC and its Guidance. Prior to issuing a safety license for export, STUK inspector request a consent from the point of contact of destination country to ensure that

- recipient has the appropriate license to possess the source
- the country of destination has the capacity to manage the safety and security of radioactive sources

(Public) If the consent is granted and the export application is authorized, STUK notifies the point of contact of the destination country. Standard IAEA forms are used for this procedure. The IPPAS team was informed that these applications are received by normal email, secure email or by using a secure application system depending on the sender. However, these applications are not classified. These applications may contain sensitive information regarding the consignor and the consignee, location of the HASS, etc.

(Public) The IPPAS team was informed that transport of category 1 and 2 sources requires a license and security plan approved by STUK. For transport see more in chapter X.10. The IPPAS team was informed that if needed a security expert from STO is involved into the authorization of export and import.

(Public) In accordance with Section 76 of the Radiation Act (859/2018) provisions exist for the return of sealed sources to the manufacturer.

(Public) Provisions exists for prior and post notifications to the relevant competent authorities. Exports are authorized by STUK after an assessment of technical and administrative capabilities are established in the receiving country.

(Public) In summary the IPPAS team noted that STUK is on its way to fully implementing the security provisions of the IAEA CoC.

X.10 Security of Radioactive Material in Transport

X.10.1 Transport Security Requirements and Regulations

(Public) The Act on the Transport of Dangerous Goods (719/1994) applies for all classes of dangerous goods (Class 1-9) including radioactive materials (Class 7). It covers all modes of transport. STUK has the regulatory oversight for the transport of Class 7 materials.

(Public) The IPPAS team was informed that the Act on the Transport of Dangerous Goods (719/1994) is under revision. The new Act will be published next year (2023). STUK is actively involved in the consultation process and will propose amendments to TRAFICOM.

[REDACTED]

(Public) The specific requirements for the transport of radioactive materials are included in Section 49 paragraph 6 of the Radiation Act (859/2018). These requirements apply to licensees that transport HASS by road and/or by rail. For HASS, STUK approves a transport safety licence as part of the licensing application. Safety licenses issued under the Radiation Act (859/2018) for road and rail transport activities of HASS are in several cases approvals valid until further notice. For reasons justified during the application process, a temporary safety license may also be granted for these transport operations.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public) STUK may conduct joint inspection with representatives of TRAFICOM. STUK can initiate inspections on its own related to the transport of HASS. STUK inspectors receive awareness training approximately every three years on the transport of dangerous goods. This training covers the basics of Class 7 transportation and includes basics for security and safety arrangements. The IPPAS team was informed that there is no specific internal transport security training or guidance for the inspectors of STO.

(Public) Basis NSS No. 27-G, para 3.43: “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.”

(Public) NSS No. 31-G, para 3.8: “A well-trained workforce is needed for an organization to meet its nuclear security responsibilities and to contribute to an effective nuclear security regime.”

(Public) **Suggestion 17:** STUK should consider establishing an internal training course for the security of radioactive materials during transport for STUK inspectors who are involved with the licensing and inspections of HASS transport.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) The prescriptive security arrangements described in the Transport security guidance are based on the ADR Chapter 1.10 and previous version of NSS No. 9.

(Public) The security arrangements are determined on the basis of UN number and the activity of the radioactive substance transported. There are three levels of security, based on the graded approach, in table 6 below:

STUK levels of security	UN and IAEA NSS No. 9-G (Rev. 1) levels
No special security arrangements (e.g. Normal business practices are adequate)	Prudent management practices
Normal security level	Basic Security Level
Security for HASS	Enhanced Security Level
	Additional security measures (for special circumstances)

(Public) Table 6: Transport security level established by STUK

(Public) The IPPAS team noted that these security levels are not fully aligned with the UN terminology and IAEA NSS No. 9-G (Rev.1) guidance for the transport of Class 7 dangerous goods.

(Public) The transport categories and security arrangements for HASS are specified in the TRAFICOM regulation (TRAFICOM/443227/03.04.03.00/2020). Nuclides specific limits for HASS activity values can be found in STUK regulation (S/5/2019).

X.10.2 Security Management and Transport Security Plan

(Public) In the licence application, the licensee must describe their management system, training and actions to maintain a good safety (security) culture. In addition, the licensee must describe the administrative, organizational and security arrangements. (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) According to the Act on the Transport of Dangerous Goods (719/1994) Section 11 paragraph d, a transport security plan is required for the transport of high-risk radioactive materials listed in 1.10.3.1.3 of the TRAFICOM Regulation. For operators transporting high activity sealed sources according to the Radiation Act, a security plan is required during the processing of the license application and in connection with other operational controls.

(Public) The IPPAS team observed that there are no provisions for additional security measures and increased threat level scenarios.

[REDACTED]

(Public)Basis: NSS No. 14, para. 4.34: “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.”

(Public)Basis: NSS No. 14, para. 4.35: “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.”

(Public)Recommendation 16: STUK should establish requirements for measures to address an increased threat level during transport and the transport security recommended measures in NSS No. 9-G (Rev.1).

(Public)The IPPAS team observed that there are no specific requirements against sabotage.

(Public)Basis: NSS No. 14, para. 4.36: “When establishing security measures to protect against a malicious act particularly sabotage, the safety features of the design of the transport package, container and conveyance should be taken into account.”

(Public)Basis: NSS No. 14, para. 4.37: “ If the current or potential threat warrants additional security measures to protect against sabotage, consideration should be given to:

- Postponing the shipment;
- Rerouting the shipment to avoid high threat areas;
- Enhancing the robustness of the package or the vehicle;
- Enhancing route surveillance to observe the current environment;
- Providing (additional) escorts or guards.”

(Public)Recommendation 17: STUK should revise the regulatory framework for the transport security of radioactive sources to include security measures against sabotage.

X.10.3 Implemented Detection, Delay and Response Measures

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public)A sample content of the security plan is an appendix of the transport security guidance. The IPPAS team noted that the content of the transport security plan is not fully aligned with IAEA NSS No. 9-G (Rev. 1).

[REDACTED]

[REDACTED]

(Public)Basis NSS No. 9-G (Rev.1), para 2.29, point (b): “The responsibilities of the regulatory body with respect to transport security should include the following:

(b) Establishing requirements **for the content** and submission of **transport security plans**, [...]”

(Public)NSS No. 9-G (Rev.1), para 2.22, point (c): “In addition, to address the secure transport of radioactive material, the national legislative and regulatory framework should do the following, in accordance with a graded approach and where applicable:

(c) Prescribe requirements for the design and evaluation of the transport security system by the shipper and carrier, as appropriate.”

(Public)Suggestion 19: STUK should consider revising the transport security guidance to differentiate the security functions (deterrence, detection, delay and response) and clarify the requirements, recommendations and guidance and to align the transport security plan content with NSS No. 9-G (Rev.1).

X.10.4 International Transport

(Restricted: [Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)](#)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

XI. FACILITY LEVEL REVIEW

XI.1 Turku University Hospital Laboratory (Tykslab)

(Public) Tykslab provides expertise and laboratory services to health care professionals and several health care centers in Southwest region of Finland. It is largest hospital in the District of Southwest Finland.

As part of the mission, the IPPAS team visited the [REDACTED]

[REDACTED] [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

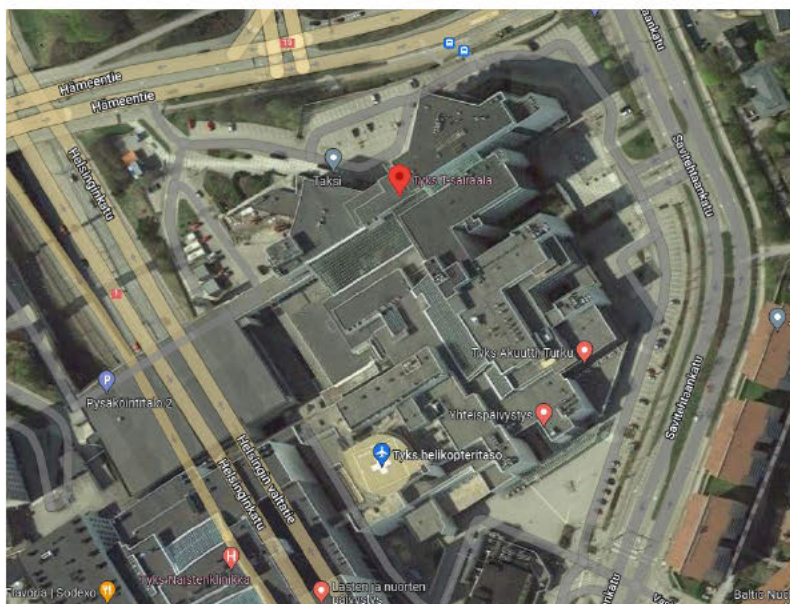


Fig. 19: Google view of Tykslab in Turku



Fig. 20: Main public entrance to Tykslab

Fig. 21: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Fig. 22: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[REDACTED]

[REDACTED]

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Fig. 23: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Fig. 24: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

XI.1.1 Security Management

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[Redacted content]

XI.1.1.1 Graded Protection and Defence in Depth

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[Redacted content]

XI.1.1.2 Trustworthiness Verification

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[Redacted content]

[Redacted content]

[Redacted content]

XI.1.1.3 Protection of Sensitive Information

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

XI.1.1.4 Security Plan

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

XI.1.1.5 Contingency Plan

Refer to chapter XI.1.2.4. on response

XI.1.1.6 Reporting Security Events

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

For reporting and response see more in chapter X.7. and XI.1.2.4.

XI.1.1.7 Location and Recovery of Missing/Stolen Material

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

XI.1.1.8 Measures to Mitigate/Minimize Radiological Consequences of Sabotage

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

XI.1.2 Security System

XI.1.2.1 Detection and Alarm Assessment

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 25: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 26: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 27: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))



XI.1.2.2 Access Control

Fig. 28: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

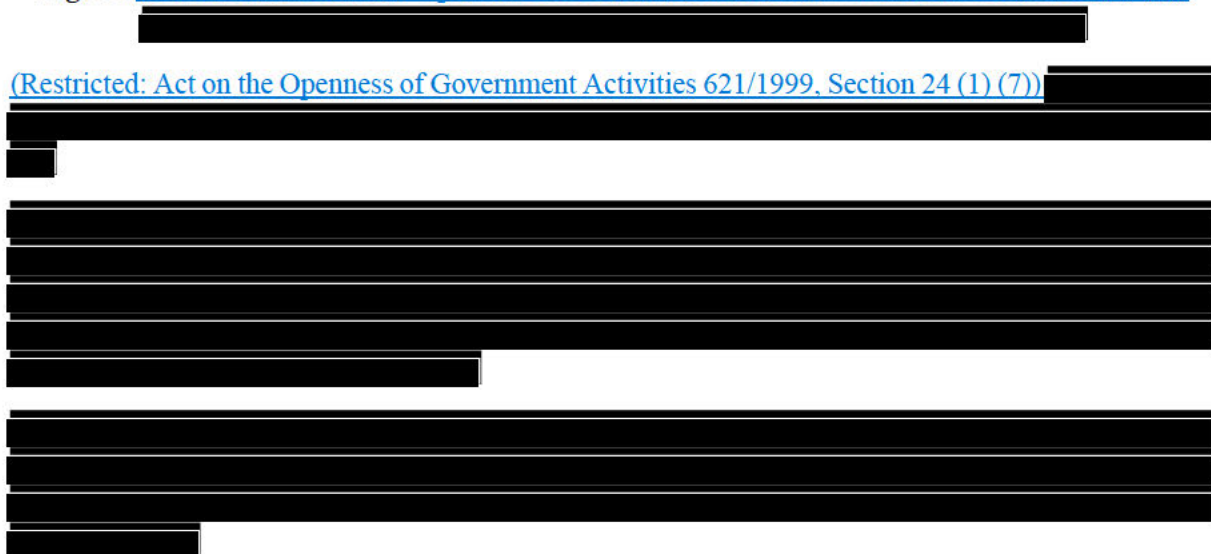
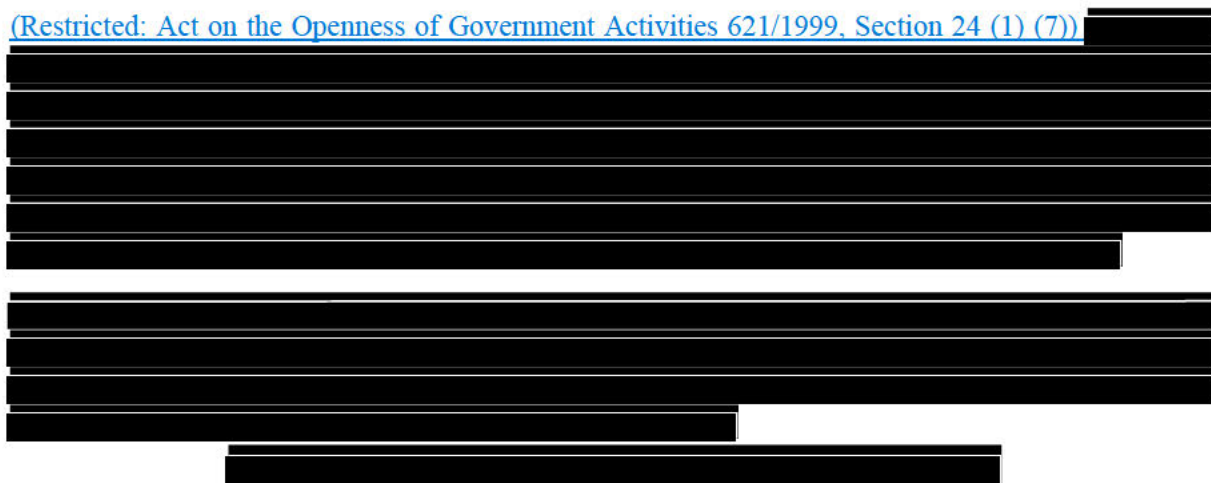


Fig. 29: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Fig. 30: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)



XI.1.2.3 Delay

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 31: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 32: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 33: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

Fig. 34: (Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

XI.1.2.4 Response

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(7) [REDACTED]

[REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

[illegible]

[REDACTED]

XI.1.2.5 Emergency Power Supply

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

XI.1.2.6 Locks and Keys

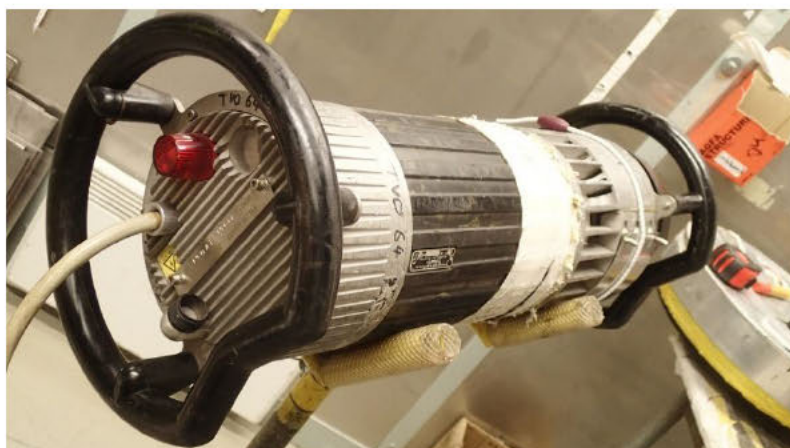
[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)


XI.2 Olkiluoto NPP

[\(Public\)](#) During the IPPAS mission, the IPPAS team visited two areas inside the OL3 NPP protected area where HASS are used and stored. OL3 also has very small activity sources. The first area is located inside the main reactor building.

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[\(Public\)](#) The second area visited used X-ray radiation devices (Andrex smart 225 that can generate 225 Kv) for non-destructive testing (NDT). The NDT laboratory is located outside the reactor building. OL3 has several mobile X-ray devices under their safety licence (approximately 13) (see figure 36).




*(Public) Fig. 36: Mobile X-ray device used for non-destructive testing
classified security level B under STUK regulations*

XI.2.1 Security Management

XI.2.1.1 Graded Protection and Defence in Depth

(Public) There are several layers of security measures that provide a very robust defense in depth against external adversaries. To prevent insider threats, the operator implemented additional administrative and technical measures.

(Public) **Good Practice 9:** OL3 implemented multiple, diverse and redundant physical barriers, access control measures and administrative security measures that provide a robust defence in depth.

XI.2.1.2 Trustworthiness Verification

(Public) See measures described in module 2 section IX.1.8

XI.2.1.3 Protection of Sensitive Information

(Public) See measures described in module 2 section IX.1.2.

XI.2.1.4 Security Plan

(Public) A security plan for radioactive sources used at OL3 was provided to STUK STO for review and approval. The plan was approved and inspected by STUK in 2019.

XI.2.1.5 Contingency Plan

(Public) See measures described in IX.1.2.

XI.2.1.6 Reporting Security Event

(Public) See measures described in module 2 section IX.2.

XI.2.1.7 Location and Recovery of Missing/Stolen Material

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1)) 




XI.2.1.8 Measures to Mitigate/Minimize Radiological Consequences of Sabotage

(Public) See measures described in module 2 section IX.2

XI.2.2 Security System

XI.2.2.1 Detection and Alarm Assessment

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) 





(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Fig. 37:

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Good Practice**
10:

XI.2.2.2 Access Control

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

[REDACTED]

(Confidential: Act on the Openness of
Government Activities 621/1999,
Section 24 (1) (7))Fig. 38:

[REDACTED]

(Confidential: Act on the Openness of
Government Activities 621/1999,
Section 24 (1) (7))Fig. 39:

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))
[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))Fig. 40:

[REDACTED]

XI.2.2.3 Delay

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))
[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))
[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

XI.2.2.4 Response

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

XI.2.2.5 Emergency Power Supply

(Public) See measures described in module 2 section IX.2.

XI.2.2.6 Locks and Keys

(Public) See measures described in module 2 section IX.2.

[REDACTED]

COMPUTER SECURITY REVIEW (MODULE 5)

XII. COMPUTER SECURITY STATE LEVEL REVIEW

XII.1 Legal and regulatory framework

(Public) The tasks of STUK are based on *NEA (990/1987)* and the *NED (161/1988)* with regard to information security.

(Public) As an authority, STUK is also bound by other Finnish legislation, the most important of which are *Act on Information Management in Public Administration (906/2019)*, *Act on the Openness of Government Activities (621/1999)* and the *Security Clearance Act (726/2014)*. These Acts are binding on the authority but not on the operators or other non-governmental organizations (see VII.3).

(Public) The main requirement regarding computer security is provided by *STUK Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020)*. The few cyber security specific regulations contained within STUK Y/3/2020 are referenced in their entirety below;

(Public) General Planning of the use of nuclear energy (Chapter 2, Section 4)

5. Appropriate information/cyber security principles shall be used in the design and maintenance of systems and components. Appropriate methods and related plans shall be in place for detecting and preventing unauthorized action targeted towards systems and components that are important to safety and information/cyber security deviations, as well as for limiting their detrimental consequences.

6. In the use of nuclear energy, preparations shall be made for managing abnormal situations arising from information/cyber security threats.

(Public) Implementation of security arrangements, and maintenance of security (Chapter 2, Section 6)

7. Information/cyber security shall be monitored with appropriate procedures to detect, prevent and analyze abnormal events and to control their consequences.

(Public) In lieu of comprehensive regulation, STUK has created a thoughtful Guidance Publication, STUK YVL A.12, *Information Security Management of a Nuclear Facility* [12.02.2021], where it states clearly in the introduction that “*This guide sets out requirements for the management of information security at a nuclear facility, and it specifies in more detail the design requirements set forth in the STUK Regulation on Security in the USE of Nuclear Energy (STUK Y/3/2020).*”

(Public) While this definition attempts to address the existence of “requirements” within a “Guide”, the overall effect is one of legal ambiguity and not well suited for use in contract enforcement with a licensee.

(Public) The IPPAS team reviewed the *YVL A.12 Guide*. The team noted that *requirements* provided in that guidance are of high level that does not allow for appropriate assessment by STUK, and although not legally enforceable, the contents of this guide do provide an additional step toward comprehensive regulation.

(Public) There are multiple areas where the existing regulations lack specificity related to key aspects of an effective nuclear cyber program, especially for an nuclear power site dependent upon modern digital controls such as that at OL3. The table below identifies many of these areas and denotes their existence where applicable within either STUK Y/3/2020 regulations and or STUK YVL A.12 guidance.

Topic	Y/3/2020	YVL A.12
Cyber security measures must be consistent with the current threat assessment or Design Basis Threat	N	Y
Digital Systems associated with Emergency Preparedness	N	Y
Conduct of a comprehensive analysis of all digital computer and communication systems and networks to identify those assets that constitute a “Sensitive Digital Asset” (SDA) or equivalent. SDA, as defined in IAEA NSS No. 42-G, is “Those digital devices whose compromise can directly affect performance of nuclear security functions or nuclear safety functions.”	N	Y
Establish effective “Defence in Depth” strategies and implementation procedures for SDAs.	N	N
Ensure that all facility personnel and contractors are aware of cyber security requirements and trained as necessary to execute their duties in a compliant manner.	N	Y
Ensure that all modifications to existing digital devices designated as SDA’s undergo a cyber-risk assessment prior to implementation.	N	Y
Generate a comprehensive facility cyber security plan that addresses how the licensee will address all aspects of the stated requirements. * YVL A.12 references an Information Security Management System as per ISO 27000 which while originally not intended for use in control centric environments may be sufficient depending upon how it is implemented.	N	*
Identify and track the configuration, known vulnerabilities and revisions of all software and hardware components designated as SDAs and or those sub platforms and networks that they are dependent upon.	N	N
Implement an effective program to track and identify emerging cyber threats as they pertain to SDAs, validate the effectiveness of existing controls and or implement new controls as necessary to maintain defence in depth across key systems and secondary support environments.	N	N
Provide for integrated incident response capability concerning timely detection, consequence mitigation, correction of	N	N

vulnerabilities and restoration / validation of impacted systems across the enterprise.		
---	--	--

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

(Public)Recommendation 18: In order to protect computer based systems that are used for physical protection, nuclear safety and nuclear material accountancy and control, STUK should review the cyber security specific contents of Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020). STUK should also consider enhancing them to be in line with commonly accepted international guidance. As a start consider a refinement and migration of those recommendations listed in the table above that are resident within STUK YVL A.12 into STUK Y/3/2020.

(Public)NSS No. 42-G is a worthwhile reference for this effort.

XII.2 Roles and responsibilities of competent authorities

(Public)The IPPAS teams was presented with a vast array of organizations that participated in the national cyber security capability for Finland, listed below are a few that appear to be most involved with areas that have high potential for interaction with Nuclear Security activities, STUK and or the licensee.

- STUK
- SUPO
- Radiation and Nuclear Safety Authority
 - o coordinates the Nuclear Information Sharing and Analysis Center (ISAC)
- TRAFICOM provides the National Cyber Security Strategy
 - o National Cyber Security Center (NSCS-FI)
 - Cyber Emergency Response Team (CERT-FI)
 - coordinates the Virtual Incident Response Team (VIRT)
 - Provides the HAVARO service
 - *KyberVPK – Community Cyber response force / hacker collective

(Public)*The KyberVPK does not appear to be an actual federal organization but rather a public volunteer group that works in coordination with the Federal organizations.

(Public)The National Cyber Security Centre, within TRAFICOM, maintains the cyber situation in Finland and regularly reports vulnerability bulletins to stakeholders through the CERT-FI. The IPPAS team was informed, that TRAFICOM’s support for nuclear security is not clearly defined or well understood, but that they are a good cyber resource when team members have a technical question that they require assistance with.

[REDACTED]

(Public)Basis NSS No. 42G, para I-12: “The State should develop a computer security strategy that supports its nuclear security regime.”

(Public)NSS No. 42G, para I-13: “The State should designate and empower competent authorities with responsibility in the development and implementation of the legislative and regulatory framework for computer security that supports the nuclear security regime. The competent authority for computer security may be different from the competent authority (or competent authorities) for other aspects of nuclear security.”

(Public)NSS No. 42G, para I-14: “The State should ensure that functions, roles, and other provisions for computer security are defined and closely coordinated between and within all competent authorities involved in nuclear security.”

(Public)Suggestion 26: The state should consider ensuring that its National Cyber Security Centre supports the nuclear security regime and establish arrangements for cooperation to support STUK’s responsibilities and duties for computer security within nuclear facilities.

(Public)The IPPAS team was informed that for computer security STUK has only one inspector with significant capabilities. If that inspector were to be unavailable or to quit, STUK would not have any significant capability.

(Public)Basis NSS No. 13, para 3.56: “The State should establish a sustainability program to ensure that its physical protection regime is sustained and effective in the long term by committing the necessary resources.”

(Public)Recommendation 19: STUK should consider developing capabilities regarding computer security and train additional experts or consider getting support from other competent authorities.

XIII. COMPUTER SECURITY FACILITY LEVEL REVIEW

(Public)In accordance with the Radiation and Nuclear Safety Authorities decision, regulation STUK Y/3/2020, Radiation and Nuclear Safety Authority’s Regulation on Security in the Use of Nuclear Energy, has been decreed by virtue of Section 7 q(1)(22) of the NEA (990/1987) as laid down in Act (964/2020)

(Public)Pertaining to the implementation of Cyber Security programs at Finnish Nuclear facilities, the regulations contained within STUK Y/3/2020 are then expounded upon in the STUK YVL series A.12 Information Security Management of a Nuclear Facility 12.02.2021.

XIII.1 Computer Security at Olkiluoto NPP

(Public)Taking into consideration the requirements and guidance provided within STUK Y/3/2020 and YVL A.12, the licensee has implemented a computer security program. During the construction phases, the Licensee also oversees Areva’s efforts to provision computer security across the Instrumentation and Control (I&C) system environments and will subsequently add that scope of work to their area of responsibilities as the contract comes to an end.

[REDACTED]

XIII.1.1 Computer Security Policy

(Public) Computer security policy represents the overarching requirements as provided through the State regulatory framework and is instrumental in the construction of the facility computer security plan and associated procedures, system implementations and resulting cyber security culture.

XIII.1.2 Asset Management

(Public) STUK YVL A.12 states, “The assets to be protected shall be identified and defined in sufficient detail.” [2021-02-12] followed by, “The threats, vulnerabilities and effects of information security events related to the assets to be protected shall be analyzed, and the necessary controls shall be defined based upon them.” [2021-02-12] In response, a rudimentary Asset Management System has been approved for deployment within the I&C environments and is addressed within PP 8.3 project Procedure IT Security Management Plan. Included plan templates indicate basic configuration information is identified and documented for all devices.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) The achievement of defense-in-depth in a computer security architecture depends upon detailed vulnerability analysis and subsequent security controls assigned at multiple layers of the operational environment. A flat security posture, although easier to implement, is much easier for an attacker to understand and compromise.

(Public) Basis NSS No. 42G, para 2-17: “The appropriate definition of what constitutes an SDA, of its extent, boundaries and interfaces, and of acceptable degrees of dependence upon other digital assets, are key aspects of creating a secure design, calling for expert judgment guided by computer security and systems engineering principles.”

(Public) Suggestion 27: In the spirit of continuous improvement, and in order to protect computer based systems used for physical protection, nuclear safety, and nuclear material accountancy against evolving threat, TVO should consider enhancing the existing computer security program to include additional aspects of nuclear cyber norms across the whole of the enterprise and I&C computing environments.

(Public) note: Examples for reference and consideration include; IAEA NSS No. 42-G; US Reg Guide 5.71 / Draft guide 5061, and the affiliated National Institute of Standards and Technology (NIST) SP 800-82r2 and NIST SP 800-53r5 or finally the NEI Milestones 08 and 09. All of these efforts to address current nuclear specific cyber threat have been developed in a cooperative fashion within the nuclear community and strive to achieve successful protection in as effective and efficient a means as possible.

XIII.1.3 Physical Protection and Environmental Security

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) Basis NSS No. 42G, para 5.26: “The application of computer security measures should be based upon a risk informed approach. The competent authority for computer security should define a risk assessment method or sequence of methods by which responsible organizations do the following:

(b) Determine whether each digital asset is an SDA

(c) Perform a computer security risk analysis to determine the required strength of computer security measures for that SDA or other digital asset...”

(Public) NSS No. 42G, para 5.29: “The risk assessment should consider all aspects of security collectively in order to address blended attacks, which can combine physical protection (including personnel, especially insiders) and computer security cyber-attacks.”

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) Suggestion 28:

XIII.1.4 Computer Operations Management

(Public) Computer Operations Management is a broad area that requires considerably more time than the IPPAS mission has to develop a comprehensive review. Initial discussions left a few impressions worthy of mention.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Suggestion**
29: [REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Public) Configuration and access control can be a serious challenge in the I&C environment, resulting in serious consequences when inappropriate media is utilized for an update or changes are made without the proper review.

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) **Good Practice**

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public)Basis NSS No. 42G, para 6.20: “The competent authority for computer security should require competent authorities and operators to develop, implement and exercise computer security procedures for the prevention and detection of and response to computer security incidents.”

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7))Suggestion 30: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

XIII.1.8 Continuity Management

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 (1) (7)) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Public)Note: Areva cyber security personnel did not take part in the visit to Olkiluoto or in the presentations at STUK.

[REDACTED]

[REDACTED]

| [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

| [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)**Suggestion**

31: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ACKNOWLEDGEMENTS

(Public) The IPPAS team received outstanding cooperation from personnel at all management, technical and administrative levels. Practical arrangements for the conduct of the mission made by the STUK, TVO and Olkiluoto NPP were excellent. Throughout the mission, personnel of STUK, TVO and all other organizations involved, cooperated whole-heartedly with the IPPAS team, generously giving their time, relevant information and kind hospitality. Such helpful assistance and the timely provision of relevant information ensured the mission was a success. Moreover, the exchange of technical knowledge and experience between the team members and host country's counterparts was mutually beneficial. Additionally, notwithstanding the need to exercise discretion with regard to all mission-related information, the team appreciated the transparency displayed by those involved in discussing sensitive matters.

APPENDIX I: SYNOPSIS OF RECOMMENDATIONS, SUGGESTIONS AND GOOD PRACTICES

Module 1

(Public) Recommendation 1: The State should amend the necessary legislation in order to implement into the national legislation the categorization of nuclear material in line with NSS 13.

(Public) Recommendation 2: To eliminate the ambiguity and to ensure that security measures do not compromise safety and safety measures do not compromise security, legislation should clearly express which cases address only safety, which cases address both safety and security and which cases address only security issues.

(Public) Recommendation 3: The categorization table (currently provided in Table 2 of YVL A.11) should be amended to be consistent with the total plutonium mass thresholds provided in Table 1 of the NSS No. 13.

(Public) Recommendation 4: The graded approach relating to the risk of unauthorized removal of nuclear material should be based on the categorization of nuclear material as provided in NSS No. 13. In particular, the security zones, the definition of which should be based on the risk of theft, should be defined based on the category of the nuclear material they might contain.

(Public) Recommendation 5: STUK should define a consistent and systematic methodology for the conduct of the vital area identification process.

(Public) Recommendation 6: STUK should give due priority and promote nuclear security culture and integrate nuclear security culture in the management system.

(Public) Suggestion 1: The State should consider revising the enabling clause in section 7r of the NEA with the purpose of clarification the legal status of the guidance documents. In order to do so, the State should consider abrogating this provision and transfer legally binding requirements from guidance documents into the STUK regulations.

(Public) Suggestion 2: The State should consider expanding the membership of the Advisory Commission on Nuclear Security and include other authorities to enhance its capabilities to address computer security related issues.

(Public) Suggestion 3: STUK should consider developing guidance to provide for a systematic approach for assessing the effectiveness of nuclear security system.

(Public) Suggestion 4: STUK should consider hosting a training course regarding the methodology to be used for the vital area identification. The content of this course could be based on NSS No. 16.

(Public) Suggestion 5: STUK should consider developing a classification and protection scheme specifically for nuclear sensitive information applicable to operators, including for “unofficial documents”, in order to have one overarching system applicable to all relevant organisations.

Suggestion 6: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[REDACTED]

Good Practice 1: The law requires the prosecutor to request an opinion from the regulatory body prior to bringing charges for offences enumerated in the nuclear and radiation legislation before the court of law.

Good Practice 2: There is a clear, detailed and extensive list of competencies, rights and powers of nuclear security officers in national legislation including the right to take action against the use of an remotely piloted (or programmed) aircraft system (RPAS).

Good Practice 3: STUK as the competent authority has established and maintains several mechanisms allowing for close internal cooperation between the STUK's entity in charge of security and STUK's entities in charge of safety and safeguards.

Good Practice 4: the Advisory Commission on Nuclear Security is established by the law, supports and provides advice to other competent authorities including STUK. Its duties cover security assessment of nuclear facilities, laws, regulations and guidance, threat assessment, cooperation and suggestions to competent authorities. Operators can attend these meeting as observers.

Module 2

Recommendation 7: [\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Recommendation 8: [\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Recommendation 9: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Recommendation 10: [\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Recommendation 11: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Recommendation 12: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

Suggestion 7: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 8: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 9: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 10: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 11: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Good Practice 5: [\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Good Practice 6: [\(Confidential: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Module 4

[\(Public\)](#) **Recommendation 13:** STUK should clarify and revise the security requirements that are set out in the security guide and in the regulation S/9/2021 to include new security requirements for information security, trustworthiness, security awareness training, frequency of verification and response arrangements to align with NSS No. 14.

Recommendation 14: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[\(Public\)](#) **Recommendation 15:** The State should ensure that STUK has sufficient human and financial resources to:

- train inspectors on the security of radioactive materials,
- conduct security inspections for HASS use, storage and transport following a graded approach and

- develop a long term plan for human resource development.

(Public) Recommendation 16: STUK should establish requirements for measures to address an increased threat level during transport and the transport security recommended measures in NSS No. 9-G (Rev.1).

(Public) Recommendation 17: STUK should revise the regulatory framework for the transport security of radioactive sources to include security measures against sabotage.

(Public) Suggestion 12: STUK should develop an internal process to ensure the timely and consistent review of security plans. This process should be tied to the authorization and licensing process and should include the protection of sensitive information (e.g. security plan, security inspection reports and deficiencies).

(Public) Suggestion 13: STUK should consider adding and also revising requirements for the maintenance and testing of security measures and update the content of the security plan based on NSS No. 11-G.

Suggestion 14: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 15: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

(Public) Suggestion 16: STUK should consider including a requirement in the regulation S/9/2021 to ensure licensees with security levels A and B implement measures to ensure a timely and effective response to attempted or actual malicious acts involving HASS.

(Public) Suggestion 17: STUK should consider establishing an internal training course for the security of radioactive materials during transport for STUK inspectors who are involved with the licensing and inspections of HASS transport.

Suggestion 18: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

(Public) Suggestion 19: STUK should consider revising the transport security guidance to differentiate the security functions (deterrence, detection, delay and response) and clarify the requirements, recommendations and guidance and to align the transport security plan content with NSS No. 9-G (Rev.1).

Suggestion 20: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

[REDACTED]

Suggestion 21: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Suggestion 22: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Suggestion 23: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Suggestion 24: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

Suggestion 25: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[\(Public\)](#) **Suggestion 26:** The state should consider ensuring that its National Cyber Security Centre supports the nuclear security regime and establish arrangements for cooperation to support STUK's responsibilities and duties for computer security within nuclear facilities.

[\(Public\)](#) **Good Practice 7:** STUK provides a list of high risk source locations to the police on an annual basis with relevant information on the material attractiveness and associated risks to support first responders safety and prioritise rapid response.

Good Practice 8: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[\(Public\)](#) **Good Practice 9:** OL3 implemented multiple, diverse and redundant physical barriers, access control measures and administrative security measures that provide a robust defence in depth.

Good Practice 10: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#) [REDACTED]

[REDACTED]

Module 5

(Public) Recommendation 18: In order to protect computer based systems that are used for physical protection, nuclear safety and nuclear material accountancy and control, STUK should review the cyber security specific contents of Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020). STUK should also consider enhancing them to be in line with commonly accepted international guidance. As a start consider a refinement and migration of those recommendations listed in the table above that are resident within STUK YVL A.12 into STUK Y/3/2020.

(Public) Recommendation 19: STUK should consider developing capabilities regarding computer security and train additional experts or consider getting support from other competent authorities.

(Public) Suggestion 27: In the spirit of continuous improvement, and in order to protect computer based systems used for physical protection, nuclear safety, and nuclear material accountancy against evolving threat, TVO should consider enhancing the existing computer security program to include additional aspects of nuclear cyber norms across the whole of the enterprise and I&C computing environments.

Suggestion 28: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 29: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 30: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Suggestion 31: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Good Practice 11: [\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

APPENDIX II: IPPAS TEAM COMPOSITION

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

██████████ IPPAS Team Leader), Swiss Federal Nuclear Safety Inspectorate (ENSI), Switzerland

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

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

██████████ Hungarian Atomic Energy Authority (HAEA), Hungary

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

██████████ Ministry of Ecological Transition (MTES), France

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

██████████ Nuclear Regulation Authority (NRA), Japan

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

Technical Coordinator

██████████ IAEA

APPENDIX III: HOST COUNTRY COUNTERPARTS

Representatives of STUK

Nuclear Security Section (YTS)

[\(Restricted: Act on the Openness of Government Activities 621/1999, Section 24 \(1\) \(7\)\)](#)

Tapani Hack	Section Head
[REDACTED]	Principal Advisor
[REDACTED]	Inspector
[REDACTED]	Inspector
[REDACTED]	Senior Inspector (virtually)
Ronnie Olander	Principal Advisor

Radiation in Industry and Occupational Exposure (TAV)

Tuomas Siru	Inspector
Antti Takkinen	Inspector
[REDACTED]	Inspector (import and export)

Legal Unit (LAS)

Ville Haataja	Head of Unit
---------------	--------------

Emergency Preparedness Unit (VAP)

Jyrki Heinonen	Chief of Preparedness
Jukka Kupila	Principal Advisor

Other STUK Representatives

Petteri Tiippana	Director General
Tapani Virolainen	Director (Nuclear Reactor Regulation)

TVO / Olkiluoto NPP

[REDACTED]	Security Manager
[REDACTED]	Safety Chief Engineer (for OL3 Unit)
[REDACTED]	Guard Manager (Securitas)

Tykslab

[REDACTED]

[REDACTED]

[REDACTED] Hospital Physicist

[REDACTED] Medical Physicist

Representatives of other Finnish Organizations Involved in Nuclear Security

[\(Restricted: Act on the
Openness of Government
Activities 621/1999,
Section 24 \(1\) \(7\)\)](#)

[REDACTED] Director of Unit (MoD)

[REDACTED] Lieutenant (Finnish Defence Forces)

[REDACTED] Senior Specialist (MEAE)

[REDACTED] Chief Superintendent (Ministry of the Interior)

[REDACTED] Senior Customs Officer (Finnish Customs)

[REDACTED] Senior Specialist (TRAFICOM)

[REDACTED] Major (Finnish Border Guard)

[REDACTED] Chief Superintendent (National Police Board)

[REDACTED] Senior Specialist (Finnish Security and Intelligence Service)

[REDACTED] Superintendent (Southwestern Police Department)

[REDACTED] Sergeant (Southwestern Police Department)

[REDACTED] Satakunta Hospital District

[REDACTED] Special Consultant (Rescue Authority Satakunta Rescue Services)

[REDACTED] Captain (Pori Brigade)

[REDACTED]