INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS)

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA)

Mission Report

June 2013

Prepared for the Hungarian Atomic Energy Authority

ABBREVIATIONS

1996 Act	Act CXVI of 1996 on Atomic Energy
Act on Armed Security Guard Services	Act CLIX of 1997 on Armed Security Guard Services, Nature and Field Guard Services
Act on the General Administrative Proceedings	Act CXL of 2004 on the General Rules of Administrative Proceedings and Services
CAS	Central Alarm Station
CCTV	Closed Circuit Television
CPPNM	Convention on Physical Protection of Nuclear Materials
Criminal Code	Act IV of 1978 on the Criminal Code
CSO	Cyber Security Officer
CTF	Counter Terrorist Force
DBT	Design Basis Threat
GIMC	Government Incident Management Centre
Government Decree 190/2011	Government Decree 190/2011. (IX.19.) Korm. on physical protection requirements for various application of atomic energy and the corresponding system of licensing , reporting and inspection
HAEA	Hungarian Atomic Energy Authority
HEU	Highly Enriched Uranium
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
INFCIRC/225	Information Circular 225/Revision 5 (Corrected), Nuclear Security Recommendations on the Physical Security of Nuclear Material and Nuclear Facilities
ISFS	Interim Spent Fuel Storage facility
LEU	Low Enriched Uranium
MD	Minister of Defence
MHR	Ministry of Human Resources
MI	Minister of Interior
MOX	Mixed Oxide Fuel
MRD	Minister of Rural Development
NDGDM	National Directorate General for Disaster Management
NM	Nuclear Material
NMAC	Nuclear Material Accountancy and Control
NPH	National Police Headquarters
NPHMOS	National Public Health and Medical Officer Service
NPP Paks	Nuclear Power Plant Paks
NSA	National Security Authority
NSC	Nuclear Safety Code
NSS	IAEA Nuclear Security Series
NTCA	National Tax and Customs Administration of Hungary
PWR	Pressurized Water Reactor
RAM	Radioactive Material

SUMMARY

This report presents the results of the International Physical Protection Advisory Service (IPPAS) mission conducted by the IAEA from 27 May to 7 June 2013 at the request of the Government of Hungary received on 20 June 2012 through the Hungarian Atomic Energy Authority (HAEA). General issues related to the conduct of the mission were discussed in September 2012, within the scope of the GC56 meetings. Detailed arrangements for the mission were discussed and agreed during the preparatory meeting which was conducted from 22 to 23 January 2013 in Budapest. A comprehensive advanced information package was prepared by the HAEA and provided to the IAEA, which facilitated successful preparation and conduct of the mission.

The first IPPAS mission to Hungary was conducted from 27 October to 4 November 1997, during which the review of the State's Physical Protection System for nuclear material and nuclear facilities and implementation of physical protection at the KFKI Atomic Energy Institute (AEKI) and at the Nuclear Training Reactor of the Budapest Technical University was conducted by a team of international experts from four Member States and the IAEA. At that time, the Team provided advice for enhancements based on INFCIRC/225/Rev. 3 and IAEA TECDOC 967.

Hungary was the first country which requested that the IPPAS mission include a comprehensive review of the national nuclear security regime using the new instrumental instruments and IAEA Nuclear Security Series (NSS) Guidance documents. The objectives of this IPPAS mission were to review Hungary's national physical protection regime for nuclear and other radioactive material and associated facilities and activities, as well as for related transports, and to compare the practices in Hungary with the provisions of the Convention on Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment, the IAEA NSS No. 20 "Nuclear Security Fundamentals: Objectives and Essential Elements of a State's Nuclear Security Regime", the IAEA NSS Recommendations (NSS No. 13 "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)", and "Code of Conduct on the Safety and Security of Radioactive Sources", and NSS No. 14 "Nuclear Security Recommendations on Radioactive Material and Associated Facilities") and other relevant NSS guidance documents.

The scope of the mission was very broad and included the review of Hungary's nuclear security legislative and regulatory framework, regulatory practices (licensing, inspections and enforcement) and coordination between organisations involved in physical protection. The scope of the mission also covered a review and evaluation of the physical protection systems currently in place at the Paks Nuclear Power Plant (NPP), Interim Spent Fuel Storage Facility (ISFSF), Budapest Research Reactor, Budapest Training Reactor and Radioactive Waste Treatment and Disposal Facility (RWTDF). Other facilities included locations where high activity radioactive materials are used for different applications (Institute of Oncology,

Hungarian National Metrology Institute, Agroster Irradiation Ltd. and Institute of Isotopes Co. Ltd.). In addition to facilities, physical protection during transport of nuclear and radioactive material was reviewed by the mission's Team. The interface of security with nuclear material accountancy, and cyber security associated with physical protection systems were also addressed during this mission.

A team of nine international experts with expertise in different nuclear security areas – representing six Member States and the IAEA – conducted the review. Mr Denis Flory, Deputy Director General, Head of the Nuclear Safety and Nuclear Security Department of the IAEA, opened the mission. The IPPAS team interacted with personnel of the HAEA and representatives of other governmental policy and regulatory organisations, as well as with key management and staff of the facilities and sites visited.

It was not within the scope of this mission to review Hungary's implementation of the 1997 IPPAS mission. However, based on the information provided by the HAEA and by licensees it appeared to the IPPAS mission team that all these recommendations had been addressed.

It is important to note that Hungary is adhering to all international instruments relevant to nuclear security, including the CPPNM and its 2005 Amendment (ratified by Hungary on 4 December 2008). Hungary also supports the Code of Conduct on the Safety and Security of Radioactive Sources as well as Guidance on the Import and Export of Radioactive Sources. The team noted that Hungarian legislation in the area of physical protection and security is continually updated.

It was recognised that nuclear security within Hungary has been significantly enhanced during the last several years. In particular, significant efforts were made by the HAEA and other relevant authorities amending the legislative framework for nuclear security. That includes adoption of the Governmental Decree 190/2011 (IX.19) Korm. on physical protection requirements for various applications of atomic energy and the corresponding system of licensing, reporting and inspection and the latest amendment of the Atomic Energy Act.

The amended legislative framework provides comprehensive security requirements for nuclear and other radioactive material (including radioactive waste). The amended legislative framework is fully in compliance and in some cases exceeds provisions of relevant international legal instruments and the IAEA Nuclear Security Series guidance.

The IPPAS team recognises significant efforts of relevant Hungarian authorities to address the risks related to cyber threats in their development of a legislative framework. It is understood that Act L of 2013 on the "Electronic Information Security of Central and Local Government Agencies" will enter into force on 1 July 2013.

Development and issuance by the HAEA in 2011 of a comprehensive set of regulatory guidelines relevant to nuclear security is commendable and could serve as an example for the regulatory authorities in other countries. It is important to note that the integrated approach between safety, security and material accountancy and control implemented at the HAEA establishes a robust basis for conducting its regulatory functions effectively.

The HAEA is responsible for the preparation of the national threat assessment for nuclear material, radioactive source, radioactive waste, interim store and final repository. The threat assessment serves as input to the development of a national and facility Design Basis Threats (DBT). The HAEA coordinates this work with several other governmental organisations. This is recognised by the team as a good practice for others to follow.

The IPPAS team also recognises that licensing is a joint responsibility of the HAEA and the National Police Headquarters. The role of the police in the licensing process is not common in many States, but is seen by the team as a positive measure. The HAEA has had to license a large number of operators and users based on the new legislation.

The IPPAS team recognised significant enhancements of physical protection systems at all facilities visited. Some improvements are still in progress and will be completed in near future. There are significant upgrades occurring at the Paks NPP physical protection system that will enhance detection, delay and response. Upgrades were underway at a number of the visited facilities. Along with these enhancements it is important to recognise the fact that the Budapest Research Reactor has converted from HEU to LEU which has made this facility less attractive as a theft target.

During the facilities visits the IPPAS team also identified some areas where additional enhancements could be required to increase effectiveness of the physical protection systems. These areas are addressed in this report by either recommendations or suggestions.

A total of 9 recommendations and 57 suggestions have been made while 12 good practices have been identified. Recommendations and suggestions address Central Alarm Stations, application of defence-in-depth, vehicle barriers and information and cyber security. Examples of good practices include site-specific DBTs, Guidelines on Physical Protection and the existence of a cross-organisational cyber security working group. The Team's recommendations, suggestions and good practices are listed in appendix 1.

Even though it was not specifically cited as a good practice it is evident that the police play a very important role in nuclear security in Hungary. The police are well integrated into the licensing and inspection process and provide a very important service in guarding and response.

The IPPAS team concluded that a well-established nuclear security regime exists within Hungary for all nuclear and other radioactive material including radioactive waste by

applying a common system of security levels based on defined categories and potential radiological consequences using a graded approach. Furthermore it appeared that appropriate physical protection measures are in place or are being developed at the facilities visited. The recommendations and suggestions provided in this report are intended to assist Hungary in applying the process of continued improvement in nuclear security. The large number of identified good practices at both the State and operator level might assist other States in strengthening their nuclear security regimes.

This report, containing the results of the review, is for exclusive use of the Government of Hungary who may share the report as it deems is necessary. Measures were taken to protect the confidentiality of the report and other related information.

Contents

1. INTRODUCTION

The IPPAS Programme, initiated in 1995, is a fundamental part of the International Atomic Energy Agency (IAEA) efforts to assist States to establish and maintain an effective physical protection regime of nuclear and other radioactive material and associated facilities and activities. The International Physical Protection Advisory Service (IPPAS) programme is offered to assist States, upon request, with an appraisal of their State physical protection regime. The appraisal includes a national-level review of the legal and regulatory framework, and the measures and procedures in place to execute that framework at facilities and during transport. Since 1996, 58 IPPAS missions have been conducted in 37 countries

The First IPPAS mission to Hungary was conducted from 24 October to 4 November 1997.This report presents the results of the IAEA International Physical Protection Advisory Service (IPPAS) second mission review conducted for the Hungarian Atomic Energy Authority during 27 May- 7 June 2013. That was 59th IPPAS mission conducted by IAEA.

Official request to conduct the mission was sent to the IAEA by the Director General of the HAEA on 20 June 2012 and the preparatory meeting was held from 22 to 23 January 2013 in Budapest. The programme of the preparatory meeting also included a visit to Budapest Research Reactor and To Paks NPP.

The objectives of the mission were to

- provide a review of Hungary's legal and regulatory framework for the physical protection of nuclear and other radioactive material and associated facilities, and associated activities;
- compare Hungary's compliance with obligations required by the *Convention on the Physical Protection of Nuclear Material* and its 2005 Amendment;
- compare existing procedures and practices in Hungary with the IAEA Nuclear Security Fundamentals (Nuclear Security Series (NSS) No.20 "Objectives and Essential Elements of a State's Nuclear Security Regime"), the IAEA NSS Recommendations (NSS No. 13 "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)" and NSS No. 14 "Nuclear Security Recommendations on Radioactive Material and Associated Facilities") and other relevant NSS guidance documents; and
- assess the physical protection measures in place at Paks NPP, Interim Spent Fuel Storage Facility, Budapest Research Reactor (RR), Budapest Training Reactor (TR), Radioactive Waste Treatment and Disposal Facility (RWTDF) and at several other facilities, which hold high activity radioactive sources and for related transports.

The scope of the mission included, in particular, a review of Hungary's nuclear security legislative and regulatory framework, regulatory practices (licensing, inspections and

enforcement) and coordination between organizations involved in physical protection and a review and evaluation of the physical protection systems in place at the at above mentioned facilities. The scope also included the assessment of the physical protection arrangements for transport of nuclear and other radioactive material. The interface of physical protection with nuclear material accountancy, as well as cyber security, was also addressed during the mission.

For this IPPAS mission, the IAEA assembled a nine-expert team representing six Member States and the IAEA. These experts have broad experience in physical protection system design, implementation, regulatory oversight, and nuclear legislation.

The team members of the IPPAS mission were Stephen Ortiz (team leader), Sandia National Laboratories, USA; Stephan Bayer, ASNO, Australia, David Ladsous, IRSN, France; Axel Hagemann, GRS, Germany; Aleš Škraban (legal expert), SNSA, Slovenia, Dave Clark, ONR CNS, UK, Nancy Fragoyannis, NRC, USA, Donald Dudenhoeffer (computer security expert), IAEA and Arvydas Stadalnikas (mission coordinator}, IAEA.

The IPPAS Team received and reviewed an advanced information package from the HAEA. The team gathered additional information on the legal and regulatory structure through interviews with Government officials representing the HAEA, Hungarian Police Headquarters, National Security Authority (NSA) and other relevant agencies. Also, visits were made to Paks NPP, ISFSF, Budapest RR, Budapest TR and RWTDF; as well as at several locations were high activity radioactive sources are used for different applications (Institute of Oncology, Hungarian Trade Licensing Office, Agroster Irradiation Ltd. and Institute of Isotopes Co., Ltd.).The team observed the implementation of physical protection practices and held discussions with facilities personnel. The meetings and the facilities visits also provided a forum for an informal exchange of information on physical protection practices used in other countries and the opportunity to discuss the technical aspects of implementing physical protection systems.

The IPPAS Team received outstanding cooperation from personnel at all technical and administrative levels. All participants were interested in obtaining international experience and advice on the best way to conduct their work and perform their duties. Their openness in discussing sensitive issues was appreciated and the team members are aware of the need to exercise discretion in regard to all mission-related information. The information contained in this report will be protected in accordance with IAEA policy and procedures for *Highly Confidential* information.

2. NATIONAL REVIEW OF NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL AND FACILITIES, RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES

Hungary is a parliamentary and constitutional republic, which has been a member of the European Union since 2004.

Hungary represents the typical model of division of powers into three branches. The Fundamental Law (Constitution) explicitly states that "the functioning of the Hungarian State shall be based on the principle of separation of powers" and so:

- Legislative power is exercised by the unicameral National Assembly that consists of 386 members. Members of the National Assembly are elected for four years,
- Executive power is exercised by the Government, headed by the Prime Minister, with several central and regional administrative bodies,
- The Judicial branch is independent from the executive and the legislative branch. The judiciary is comprised of independent courts, the supreme body of which is the Curia.

Hungary's Head of State is the President of the Republic, who is elected with a two-thirds majority in Parliament, and who – as a so-called "neutral branch of power" – has authority which is mainly symbolic in nature.

The Constitutional Court is the supreme body for the protection of the Fundamental Law. It can review the constitutionality of laws and regulations – either adopted by the legislative branch (Acts) or the executive branch (Decrees).

Administratively, Hungary is divided into 19 counties. In addition, the capital, Budapest, is independent of any county government. The counties are further subdivided into 174 sub-regions, and Budapest is its own sub-region. Only for statistical and development purposes the counties and City of Budapest have been grouped into seven regions.

In Hungary, Acts can be enacted by the National Assembly. The Constitution sets out the fundamental rights and obligations to be regulated by Acts. The Constitution/Fundamental Act brings further domains within the exclusive scope of legislation. The National Assembly adopts some Acts by a simple majority of votes, i.e. more than half of the votes of the Members of Parliament present, and others by a two-thirds majority (qualified majority). In addition to the Act adopting the Constitution, the Act ratifying and promulgating the international treaty on EU accession and the Act on national emblems also require a two-thirds majority of the votes of all the Members of Parliament. The acts that require a two-thirds majority of votes are specified by the Constitution.

The Constitution recognizes Government Decrees, Ministerial Decrees, and other several other types of Decrees on the State and Local level.

The *Government's authority to enact decrees* may be primary or based on legislative authorizations. The primary powers are established by Article 15/(3) of the Constitution, which declares that the Government shall issue decrees within its sphere of authority. This does not restrict the National Assembly, which may bring any regulatory field under its authority.

Under the Constitution the Government may, also under specific legislative authorization, enact decrees to implement acts. Under the provisions of the Constitution, an authorization to enact implementing regulations must specify the holder, subject and scope of the authorization. The holder may not give further legislative authorization to another party.

Ministerial Decrees are a special type of decree. They rank below the level of Government Decrees in the hierarchy of legislation. Under the Constitution, ministers may issue decrees within their sphere of responsibility/competences and on the basis of authorizations under Acts of Parliament or Government Decrees. Two conditions must therefore be met for the issue of Ministerial Decrees.

Hungary/the Government of Hungary may conclude **international agreements** with other States/the governments of other States. In Hungary the relationship between international agreements and domestic law is based on a dualist system, i.e. international agreements become part of domestic law via their promulgation by legal regulations.

The following chapter of the report covers the Team's the review of national legislation both in terms of security regime for nuclear materials as well as radioactive material and associated facilities and associated activities. This is facilitated by the fact that the current legislative framework addresses nuclear and other radioactive material in the same legislation.

With respect to the legal framework covering protection of classified information and cyber security (electronic information security) it should be noted that the review and assessment of those parts are elaborated elsewhere (see chapters on Confidentiality and Computer Security of the report)

2.1. INTERNATIONAL INSTRUMENTS

The involvement in international nuclear security-relevant instruments/activities is noted. The Hungary has signed or is a party of the following international legal instruments:

- *Treaty on Non-Proliferation of Nuclear Weapons* – promulgated by the Law-decree 12 of 1970;

- *Agreement Between the Hungarian People's Republic and the International Atomic Energy Agency for the Application of Safeguards in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons* – promulgated by the Law-decree 9 of 1972;

- *Additional Protocol to the Agreement for the Application of the Safeguards in Connection with the Treaty on Non-Proliferation of Nuclear Weapons* – promulgated by the Act XC of 1999;
- last two mentioned instruments above were suspended by Hungary and finally the trilateral *Euratom-IAEA-Hungary safeguards agreement and the additional protocol* was promulgated by Act LXXXII of 2006.

- on December 4, 2008 Hungary deposited to the IAEA its instrument of ratification of the *Amendment to the Convention on the Physical Protection of Nuclear Material*; it is to be underlined that Hungary has notified the depositary of the convention its point of contact (PoC) and the competent authority details – in both cases HAEA;

- on April 12, 2007 Hungary deposited its instrument of ratification of the *International Convention for the Suppression of Acts of Nuclear Terrorism – promulgated by the Act XX of 2007*;

Hungary has made a political commitment with regard to the *Code of Conduct on the Safety and Security of Radioactive Sources and the Supplementary Guidance on the Import and Export of Radioactive Sources.*

Hungary also complies with the:

- *UN Security Council Resolution 1540* - by which all States shall refrain from supporting non-State actors that attempt to acquire, use or transfer nuclear, chemical or biological weapons and their delivery systems - and submits the required national reports to the 1540 Committee, and
- *UN Security Council Resolution 1373* - which call on States to work together to prevent and suppress terrorist acts, - and submits the required national reports to the Counter-Terrorism Committee.

Hungary is also party to all relevant international legal instruments in the broader area of nuclear safety and radiation protection. Just to mention some of them: the *Convention on Nuclear Safety, the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, the Convention on Early Notification of a Nuclear Accident and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency*. In the area of nuclear liability, Hungary is a party to the *Convention on Civil Liability for Nuclear Damage under the auspices of the IAEA and the Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention.*

Hungary has also concluded numerous bilateral agreements with other countries on exchange of information on nuclear safety and/or radiation protection issues, on early notification in case of radiological emergency, etc.

2.2. NATIONAL LEGAL FRAMEWORK

The following chapter of the report covers the Team's the review of national legislation both in terms of security regime for nuclear materials as well as radioactive material and associated facilities and associated activities. This is facilitated by the fact that the current legislative framework addresses nuclear and other radioactive material in the same legislation.

With respect to the legal framework covering protection of classified information and cyber security (electronic information security) it should be noted that the review and assessment of those parts are elaborated elsewhere (see chapters on Confidentiality and Computer Security of the report).

2.2.1. Laws

- ***Act CXVI of 1996 on Atomic Energy***

The purpose of the Act on Atomic Energy (hereinafter referred to as "*1996 Act*") is to ensure the peaceful use of atomic energy in industrial, agricultural, health-care and scientific activities, taking into account the risks it may represent to human life and to nature, as well as the protection of the population and the environment against the hazardous effects of ionizing radiation. The Act extends over the peaceful use of atomic energy wherein the "use of atomic energy" is defined as:

> "a) activities related to nuclear or other radioactive materials,
>
> b) activities entailing ionizing radiation, and activities corresponding to facilities or equipment meant for the use of atomic energy according to Para. a)".

This Act also provides for the administrative duties and obligations of atomic energy users and of the involved authorities, and for the authorization proceedings related to the use of atomic energy. The Government, through the Hungarian Atomic Energy Agency (hereinafter referred to as "HAEA") governs and controls that atomic energy be used in a safe manner [Section 6/(2)]. Nuclear facilities must pay an "oversight fee" to the HAEA which establishes the amount of such payment. This Act also provides rules also for the storage and disposal of radioactive wastes and spent fuels, for actions to prevent extraordinary events and to mitigate eventual consequences, for the liability for damages arising from the use of atomic energy and for the reimbursement for damages caused. Chapter VI lays down provisions regarding

the National Nuclear Fund which is a separate state fund ensuring the financing of: the final disposal of radioactive wastes, the temporary storage of spent fuels, the closing of the nuclear fuel cycle and nuclear site dismantlement.

Section 11 of the *1996 Act* relates to requirements on basic security checks. Such authorization is needed for most job positions in the field of atomic energy (e.g. those employed in nuclear facilities, or by operators using, storing or transporting nuclear or Category 1-3 sealed radioactive sources). This security authorization is provided by the regionally competent police departments. The conditions for the security authorization are verified annually. The job positions having access to classified information requires additional security vetting conducted by the Constitution Protection Office. The level (i.e. scope and depth) of security vetting is in proportion to the level of classification (i.e. top secret - Level C security vetting, secret - Level B security vetting, confidential - Level A security vetting). It is worth mentioning that the HAEA plays no role in personnel security checks and security vetting.

Section 16 of the *1996 Act* covers in great details the rules of accountancy and control of radioactive and nuclear material and of the connected data supply. Based on this section of the act and corresponding powers (given in Section 17/(2) points 20 and 21) the HAEA maintains a central accountancy for radioactive materials including separately handled nuclear materials, which contains the location, physical and chemical properties of radioactive materials, the user of atomic energy and the activity pursued with the materials. Data contained in the central accountancy system may also be used for statistical purposes.

IAEA guidance NSS No.14 Para 3.10 recommends that the State should establish, develop and maintain a national register of radioactive material over thresholds defined by the State. This national register should, as a minimum, include Category 1 and 2 radioactive sealed sources, as described in the Code of Conduct on the Safety and Security of Radioactive Sources. Other radioactive material could, as appropriate, be included in this register.

Good practice 01: The national register of radioactive material, which is established and maintained by the HAEA and to which the Ministry of Human Resources has access includes not only the sources belonging to Category 1 and 2, but all the sealed radioactive sources above the exemption activity levels.

Since the HAEA is the governmental authority which is entrusted for the execution of the vast majority of the tasks indentified in this Act, Section 17 provides for very detailed listing of specific tasks. Scope of competences and tasks of other public administrations (minister responsible for health, for the police, for oversight of land use, for construction, for environmental protection, for national defence and minister responsible for education) are dealt with separately in Sections 20 to 28 of the *1996 Act*.

The *1996 Act* also contains the basic concept of nuclear security (Sections 30 to 32) and establishes the legal basis for further detailed regulation of physical protection. The Government is empowered to regulate with its decrees a whole range of areas, as detailed in Section 67, while Section 68 represents such legal basis for the different ministerial decrees.

The last revision of the *1996 Act* entered into force on August 3, 2011.

- ***Act CLIX of 1997 on Armed Security Guard Services, Nature and Field Guard Services***

The Act on Armed Security Guard Services, Nature and Field Guard Services (hereinafter referred to as: " *Act on Armed Security Guard Services*") regulates in Chapter I the facilities and activities to be protected by the armed security guards, the establishment of such services, the rights and obligations of armed security guards, and their equipment and method of operation. In Chapter II and III, the 1996 ASGS Act provides rules with regard to, respectively, ranger and rural constable service, which is obviously beyond the purpose of this report.

Based on the provision of Section 1/(1) c) the nuclear and other radioactive material as well as the activities associated with their use, manufacturing, storage, distribution and/or transport (specified by the law) fall within those activities and facilities having extreme importance for the supply of the public and are not protected by the Hungarian Air Forces, Police or by Hungarian Tax and Custom Administration ("obligant").

The Police is the authority for licensing procedures regarding ordering the establishment, operation and ceasing of the armed security guard service. Each member of the armed security guard service must be licensed. To this end he/she has to

- fulfil basic general requirements,
- successfully pass the security check,
- successfully pass a theoretical exam, and
- has to prove his/her fitness for duty.

The armed security guards under *Act on Armed Security Guard Services* require security check as well.

Based on the Annex 5 of the *Governmental Decree 329/2007(XII.13) Korm. on the Police Forces and Duties and Responsibilities of the Police*, the HAEA participate in licensing through its role of the "special authority".

The main responsibilities and duties of the Police are listed in Section 4 and in Section 5 cover the general duties of the obligant, while powers and duties of armed security guards are listed in Section 10 and 10/A as well as Section 9/A (with respect to operation of electronic

surveillance system). The requirements on cooperation of the armed security guard service with other State authorities are prescribed in Section 10/B..

- ***Act CXL of 2004 on the General Rules of Administrative Proceedings and Services***

Act CXL of 2004 on the General Rules of Administrative Procedings and Services (hereinafter referred to as: "*Act on the General Administrative Procedings*") lists those organisations that shall be regarded to have an administrative authority to carry out administrative actions. Among them there are also governmental bodies – like HAEA. This Act contains the provisions on the principles of procedures, on languages to be used, on the rights and obligations of the clients, on data procession, on the jurisdiction, on powers and authorisation of authorities, on the general rules of communication, etc. There are also provisions on general procedures regarding regulatory inspection, regarding administrative penalties, and enforcement actions. Section 19 sets the powers of authorities that shall be defined by law specifically for the various types of proceedings of the authorities. It is worth mentioning that based on Section 13 of this Act, in connection with the use of atomic energy the statutory provisions (partially or in whole) may be laid down elsewhere (i.e. *Atomic Energy Act*) in derogation from this Act.

- ***Act CXXV of 1995 on the National Security Services***

The *Act on the National Security Services* set the provisions on organisation and legal status of the national security services (i.e. civil and military security services); on duties of the national security services; on management and control of the national security services (including Parliamentary control); and on staff, basic principles of operation, measures and data management of the national security services. Among other provisions it furthermore includes provisions on intelligence information gathering, on exceptional authorisation and rules of national security protection and control.

The objective of the national security check (hereinafter referred to as "check") carried out by the National Security Services is to examine whether persons nominated to/in important and classified jobs meet the security requirements necessary for the lawful operation of public life and the national economy and, if necessary, those derived from international commitments.

The investigation of the security conditions means the detection of risk factors, circumstances, and pieces of information that could be used to make the activity of a person in an important and confidential job (as they are described in Annex 2 of the Act) vulnerable to influence for illegal purposes, and hence create a situation that could violate or threaten national security.

According to Article 69 of the *Act on the National Security Services* the competent minister initiates checks [paragraph (4) h)] of persons performing job specified by him/her pursuant to point 18 of Annex 2, while the head of secret-owning organisation initiates checks [paragraph

(13)] of the persons specified in the Article 68/(4) e) and point 19 of Annex 2. A person (expert) applying for/invited to a job/office subject to mandatory checks must be informed in advance of the possibility of being subject to security checks and the possible methods thereof, and the check could be carried out exclusively with the prior written consent of the person nominated to/performing the important and confidential job. On the basis of information and data obtained during the check, the National Security Service draws up a security expert opinion that specifies every one of the safety hazard factors that were identified and submits it to the initiator. The initiator then informs the person concerned of the termination of the check and of the contents of the security expert opinion — except under circumstances indicative of a criminal act.

- ***Act IV of 1978 on the Criminal Code***

Notwithstanding Hungary's political transition in 1989 from a former constitutional and legal system to a liberal democracy, the *Act IV of 1978 on the Criminal Code* (hereinafter referred to as "*Criminal Code*") is still in force.

The existing *Criminal Code* underwent substantial changes since 1989. There has been dozens of laws adopted to modify the *Criminal Code* and there have been many decisions of the Constitutional Court that declared *Criminal Code* provisions unconstitutional.

While Hungary deposited to the IAEA its instrument of ratification of the *Amendment to the Convention on the Physical Protection of Nuclear Material* at the end of 2008, the last revision of the *Criminal Code* took place in 2007. Before the ratification of amended CPPNM, Hungary reviewed the *Criminal Code* and the final conclusion was that there was no need for additional modification, because the *Criminal Code* as of 1/07/2007 already includes the provisions of amended Article 7.

2.2.2. Governmental and Ministerial Decrees

- ***Government Decree 190/2011. (IX.19.) Korm. on physical protection requirements for various application of atomic energy and the corresponding system of licensing, reporting and inspection***

The Government Decree on physical protection requirements for various application of atomic energy and the corresponding system of licensing, reporting and inspection (hereinafter referred to as: "*Government Decree 190/2011*") entered into force on October 4, 2011 based on Paragraphs q) and r) of Section 67 of the *1996 Act*. According to Section 31 of the Decree the HAEA is responsible for licensing and inspection of construction, operation and modification of the physical protection system of nuclear facilities, interim storage or final repository of radioactive wastes and nuclear materials, radiation sources and radioactive wastes with the involvement of the Police as special authority. *Government Decree 190/2011* covers areas, such as: national threat assessment; design basis threats; categorization (of nuclear materials, radioactive sources and radioactive waste), goals of and basic requirements for physical protection (including required physical protection levels); functions of physical

protection system (deterrence, detection, delay and response), other requirements, which include physical protection zones, nuclear security culture, insiders, access control, planning, etc. Furthermore there are also provision on licensing and inspection. Special chapter of this Decree is devoted to separate requirements for physical protection of fix and mobile equipment that generate ionizing radiation but do not contain radioactive material. According to the closing provisions:

- the HAEA establishes (within 30 days after entering into force of this Decree) a facility specific DBT – with its resolution;
- the "obligant" (licensee of a nuclear installation, interim radioactive waste storage or final radioactive waste repository, holder of a radioactive source, holder of radioactive waste and holder of nuclear material) had to submit an application to construct the physical protection system according to its physical protection plan; for those of them, who are subject of "facility specific DBT" the timeframe for submission was - not later than 6 month after the information of the resolution and for the others - not later than 6 month after the entering into force of this Decree. The same section also provides the possibility of "grace period", i.e. exemptions and permitted duration of non-compliance in relation to the provisions which are not or not fully complied with. The HAEA, in the course of consideration of the exemption and determination of the duration of non-compliance, has taken into account the decree of deviation, the scope, costs and required time of measures necessary to reach the compliance.

The *Government Decree 190/2011* represents the main and very comprehensive legally binding document in the physical protection field.

- ***Government Decree 112/2011. (VII.4.) Korm. on nuclear energy-related Term of Reference of the European Union and nuclear energy–related international obligation of the Hungarian Atomic Energy Authority, on appointment of the special authorities involved in the official procedures of the Hungarian Atomic Energy Authority, the amount of fines and the Scientific Council, assisting the work of the Hungarian Atomic Energy Authority***

This Government Decree stipulates the amount of fines, which could be charged by the HAEA in accordance with the provision of Section 15 of the *1996 Act* and lists the circumstances which have to be taken into account before a ruling. The Decree also has provisions on establishment of Scientific Council assisting the work of HAEA (advisory role in the safety as well as in non-proliferation matters); members of Scientific Council are appointed by the Minister in charge for supervision of the HAEA on the motion of the Director General of the HAEA. Furthermore Annex 1 of the Decree specifies the "special authorities" which are involved into licensing where HAEA plays a leading role and issues a final decision/license.

Suggestion 01: Relevant authorities could consider extending the mandate of the Scientific Council to cover nuclear security issues.

- ***Ministerial Decree 47/2012 (X.4.) BM on the Police Tasks in Relation to the Application of Atomic Energy***

This Decree establishes those aspects that are to be considered by the National Police Headquarters during the licensing of physical protection plans, as well as during the inspection of licensees. During the sublicensing procedure the police checks whether the application is in compliance with the *Government Decree 190/2011* requirements. During the inspection the police role is to check facility entering systems, guarding conditions, physical security and protection systems, etc. Police task is also to investigate the incidents and accidents occurring during the use of nuclear energy. The Decree also determines the police tasks in relation to transport of nuclear materials.

- ***Government Decree 329/2007(XII.13) Korm. on the Police Forces and Duties and Responsibilities of the Police***

This Decree among other things appoints (in Annex 5) the HAEA as a "special authority" within licensing process under the provisions of the *Act on Armed Security Guard Services*.

The IPPAS Team considers that ample coverage has been made in acts and associated delegated legislation (Decrees) for the obligation of the State to establish and maintain a legislative and regulatory framework to govern physical protection, as obliged by the amended CPPNM in Fundamental Principle C: *Legislative and Regulatory Framework*. The process of continuous legislative alignment to the up to date internationally recognised standards and good practices is in place through the system of amendments of the legal framework.

2.3. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

Roles and responsibilities of competent authorities engaged into the security area in Hungary are provided for in the 1996 Act (where in Section 8 and especially in Section 17 there is very detailed listing of specific tasks of the HAEA and in Section 20 to 28 the scope of competences and tasks of other public administrations). Furthermore the Police responsibilities and competences regarding armed security services in nuclear and other radioactive materials are covered in the *Act on Armed Security Guard Services*.

HAEA and the National Police Headquarters are considered as the competent authorities which are responsible for the implementation of the legislative and regulatory framework and are assigned for supervision and enforcement of relevant physical protection legislation.

According to the Section 6/(2) of the *1996 Act* and the *Act XLIII of 2010 on Central State Administration Bodies and the Status of Government Members and Secretaries of State* the HAEA is defined as a "governmental office". The later Act in Section 70 and 71 elaborates the concept of governmental office, according to which a governmental office is a central public administration body established by act under the supervision of the government. Supervision of a governmental office is performed by a minister designated by the Prime-Minister. A governmental office shall not be instructed in its legally defined competence. As

Team was explained the above stated act stipulated in its article 75/(4) that the Prime-Minister appoints by decree the "supervising" minister for different Governmental offices.

This provision of the Act has been implemented by the *Prime-Minister Resolution 5/2010(XII.23) ME*. Based on that resolution the Minister of National Development is the designated supervisor of the HAEA. Although this Ministry is covering also energy sector of the country and the HAEA reporting line to the Government and the National Assembly goes through the appointed minister, there are several provisions in the legislation which provide that the HAEA is independent from bodies responsible for developing and promoting of nuclear energy.

The first and the most important one is the one in *1996 Act* which stipulates that competent authorities (under *1996 Act*) are independent of the public administration organisations interested in promotion and development of atomic energy [Section 5/(2)]. The *1996 Act* furthermore provides in Section 8 that the HAEA decisions shall not be modified or annulled by virtue of supervision. The Team was explained that also, based on the Section 100 of the *Act on the General Administrative Procedings*, appeals against the decisions of the HAEA are not allowed and that only judicial review of such decisions is ensured.

Section 19 of the *1996 Act* stipulates that nuclear facilities under construction or in operation have to pay oversight fee to the HAEA. The Team was explained that the majority of the annual budget of the HAEA is revenues collected through the oversight fees, while the State provides only a small proportion.

Based on the recently adopted *Governmental Resolution 1007/2013 (I.10) on Transformation of the State Administration System*, since February 1, 2013 the HAEA has been operating in the new organisational structure in accordance with the Resolution to reduced the percentage of management position for 10%.

The HAEA has submitted its new Organisational and Operational Rules to the Minister of National Development for approval.

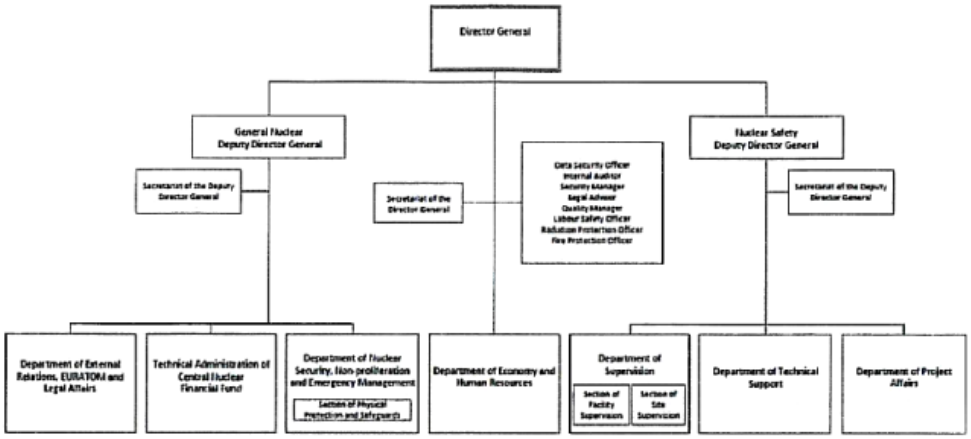

Figure 1. The organisational scheme of the HAEA

2.3.1. Licensing/Authorisation Process

The HAEA is, based on the several provisions of the *1996 Act*, the competent authority to which majority of regulatory oversight activities are entrusted. In relation to security and physical protection HAEA is supported by the NPH, as so called "special authority" (co-authority). The responsibilities and roles in licensing process of both, the HAEA and the NPH a well defined and clearly separated from one another in the legislation.

Since *1996 Act* provides only a basic concept of nuclear security the details are set forth in the Government *Decree 190/2011*, which specifies in its Section 32 the cases when the license is envisaged:

- to construct the physical protection system of nuclear facility, interim store and final repository of radioactive waste, nuclear material, radioactive source and radioactive waste according to the physical protection plan,
- to extend the license of the physical protection system of nuclear facility, interim store and final repository of radioactive waste, nuclear material, radioactive source and radioactive waste,
- to transport nuclear material, radioactive source and radioactive waste, and
- to modify a licensed physical protection system, if the modification needs modification of the physical protection plan.

Physical protection plan of nuclear facility, except for that equipped with a nuclear reactor of less than 1 MW thermal power, and used, stored and transported nuclear material, radioactive

source, and of processed, stored and transported radioactive waste shall be attached to the license application.

Based on general provision in the *1996 Act* (Section 14 - by which license may be granted for limited or unlimited duration, or bound to specific conditions) the *Government Decree 190/2011* specify that the license is valid for 5 years, except for the transport of nuclear material, radioactive source or radioactive waste requiring level A or B physical protection, when the license is valid only for the specific transport.

On the other hand for the licensing provided for in the *Act on Armed Security Guard Services* the Police is in charge. It this case, based on the Annex 5 of the *Government Decree 329/2007(XII.13) Korm. on the Police Forces and Duties and Responsibilities of the Police*, the HAEA participate in the licensing through its role of the "special authority".

The team felt that the general licensing/approval procedure as lied down in Hungarian legislation follows the INFCIRC 225, Rev. 5 – "Nuclear security recommendations on physical protection of nuclear material and nuclear facilities" and at the same time also NSS 14 – "Nuclear security recommendations on radioactive material and associated Facilities" and is in line with them.

2.3.2. Inspection, Enforcement and Penalties

The *1996 Act* has only few provisions on inspection (Section 12A), enforcement (Section 14) and penalties (Section 15); Section 67 of that Act furthermore provides for the Government to regulate by the decree:

- the rules of special enforcement procedures (which has never been adopted) and
- the rates of penalties stipulated in Section 15, which has been done through the above mentioned *Government Decree 112/2011*.

The HAEA is authorized to conduct inspections within its competence at any user of atomic energy (Section 4 of the *1996 Act*). The Inspection duties and powers are to some extent dealt with in the *Government Decree 190/2011* (Section 34). On the other hand the Team was assured that the provisions regarding regulatory inspection, administrative penalties and enforcement actions, as they are stipulated in the *Act on the General Administrative Procedings* are fully functional and meet the required and expected level of efficiency.

The fine is only one of the tools of law enforcement. Other tools to be used before or together with fining are:

- warning of the licensee and calling upon the licensee to correct a non-compliance or infringement, setting a fair deadline for correction;

- ordering the obligation and giving a deadline (prescription of the implementation of complementary measures);
- limiting the operating conditions (limitation or withdrawal of previously issued licenses and permits).

HAEA inspection activities are based on the risk informed approach. The "Inspection plan" is prepared on the quarterly basis and the frequency of the inspections is adapted to the category of sources; generally speaking the most inspections are conducted as announced; the *1996 Act* also allows so called unannounced inspections which, as the Team was told, have been used and practiced very seldom.

It is also worth noting that based on the Section 29 of the *1996 Act* the HAEA may authorize an institute (which has the necessary human and objective conditions) or a person (who has appropriate special professional qualifications) to perform inspections. Such an institute or person shall assume the same rights as the HAEA inspectors with the exception that it/he/she has no right to take measures.

In the field of inspection responsibilities of HAEA and the Police are shared. Both authorities are obliged to harmonise their inspection plans and to send their respective inspection records to each other (Section 34 of the *Government Decree 190/2011*). The Team was told that both authorities conduct the joint inspections which are more common at the nuclear facilities and holders of Category 1-2 sources.

On the other hand, based on the Section 20 of the *1996 Act*, the Ministry of Human Resources is responsible, among other tasks, for licensing and inspection of procurement, fabrication, production, possession, storage, use, application, transformation, trading of radioactive materials as well as for licensing and inspection of construction, commissioning, operation, modification, repair and liquidation of non-nuclear facilities used for activities those activities. The safety license is granted by the regional offices of the Ministry of Human Resources. Although the legislation requires the harmonization of safety, security and non-proliferation management systems (see, for example Section 18 of the *Government Decree 190/2011*), during the interview with the representatives of the HAEA the Team was explained that no such practice, as provided for the cooperation between the HAEA and the Police, is in place between the HAEA and the Ministry of Human Resources.

Basis: IAEA NSS No 14 Para 3.25:

Recognizing that both safety and security have a common aim — to protect persons, society and the environment from harmful effects of radiation — a well coordinated approach in safety and in security is mutually beneficial, the State should ensure that:

- Consultation and coordination are maintained between those responsible for safety and security to ensure efficient security of *radioactive material* and to ensure that regulatory

requirements are consistent, especially when responsibility for safety and security is assigned to different *competent authorities*;

Recommendation 01: With regard to other radioactive material, the regulatory bodies should make appropriate formal arrangements to ensure well coordinated approach between competent authorities responsible for safety and those responsible for security.

During a visit to the Emergency Response Centre, it was explained to the Team that within Emergency Response Organisation, which is set up at HAEA in case of an emergency, there is no expert/consultant for security.

Basis: INFCIRC/225/Rev 5, Para 3.58

The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration.

Suggestion 02: HAEA may consider revising its Emergency Response Plan by ensuring the presence of a security expert within Emergency Response Organisation in order that security measures during a response to a nuclear security event can also be managed from such prospective.

To ensure that safety-related compulsory prescriptions are enforced, the HAEA has elaborated an "Enforcement Policy" that is included in its overall quality assurance system and it applies this policy. HAEA through Enforcement Policy expresses its commitment to enforce compliance with effective requirements in all fields of the use of atomic energy subject to its regulatory scope of authority, and in the performance of all related activities. All users of atomic energy subject to HAEA's regulatory scope of authority are, on the other hand, expected and assumed by HAEA to act and behave in good faith and in adherence to various Act, to follow effective safety regulations on a voluntary basis, as well as to report on, investigate and rectify any irregularities that may occur since those steps are essential parts of an appropriate safety culture.

The "Enforcement Policy" is also publicly available on the HAEA website.

Rather similar enforcement tools are also on disposal to the Police when exercises its powers in relation to the *Act on Armed Security Guard Services*; in very specific circumstances [Section 4/(4)] the police may step-in and substitute unexacting armed security guard service – at the expense of the licensee.

As already explained in previous section of the this Report the HAEA cannot adopt the obligatory type of legal acts (acts, decrees) but is allowed to adopt regulatory guidelines, as non- legally binding type of legal documents. Bellow is the list of guidelines from the physical protection (security) area as adopted by HAEA and issued by the Director General of the HAEA:

- Categorization of nuclear materials, radioactive sources and radioactive wastes (PP-1),
- Detailed requirement levels for the systems, structures and components of the deterrence physical protection function (PP-2),
- Detailed requirement levels for the systems, structures and components of the detection physical protection function (PP-3),
- Detailed requirement levels for the systems, structures and components of the delay physical protection function (PP-4),
- Determination of physical protection zones (PP-5),
- Security culture (PP-6),
- Design of the physical protection system of nuclear materials, radioactive sources and radioactive wastes in use or store against unauthorized removal and sabotage (PP-7),
- Design of the physical protection system of nuclear facilities (with the exemption of those operating with a reactor having less than 1 MW thermal power) and radioactive waste temporary storage and final disposal facilities (PP-8),
- Evaluation of the effectiveness of the physical protection system of nuclear facilities (with the exemption of those operating reactor having less than 1 MW thermal power), and radioactive waste temporary storage and final disposal facilities (PP-9),
- Preparation and submittal of the physical protection license applications (PP-11),
- Physical protection related reporting system (PP-12),
- Protection against insiders (PP-13),
- Operation, maintenance and testing of physical protection systems and components (PP-14),
- Preparation of the physical protection plan required for the transport of nuclear and other radioactive materials (PP-15)
- Detailed requirement levels for the realization of the response physical protection function (PP-16).

All above listed guidelines are available on the HAEA website.

The guideline PP-10 – "Development of the DBT (Design Basis Threat) is not publicly available and is provided only to the relevant organisations), while some of them are still under preparation, as for example:

- Physical protection requirements for new nuclear power plant units (PP- 17)
- Protection of IT and ITC systems (PP-18)

In each of the guidance there is a legal explanation (in the "Preamble") of the hierarchy of security regulations: internationally obligations as accepted through ratification of different international conventions, domestic acts and decrees (Governmental and Ministerial) and guidelines. It is also explained that the recommendations in the guidelines are meant as the methods how the requirements determined in the acts and decrees should be complied with as to allow the HAEA and the licensee to proceed smoothly in the licensing and other regulatory procedures.

Furthermore each guideline contains also the reference to the text of the act and/or decree which relates to the subject of guideline in question and then provides concrete

recommendations. The references to the corresponding laws and regulations includes also internationally accepted and recognized standards (as for example those of the IAEA Nuclear Security Series).

Good practice 02: Although as legally non-binding instruments, the HAEA's guidelines represent, according to their number, structure and content, a great tool for the users to comply with the legally binding requirements by showing them the way that is most advised by the HAEA. The ongoing work on the preparation of the "Physical protection requirements for new nuclear power plant units" (PP-17) and "Protection of IT and ITC systems" (PP-18) shows orientation of the HAEA to the future objectives, roles and responsibilities.

2.4. INTEGRATION AND PARTICIPATION OF OTHER ORGANISATION

2.4.1. Other Governmental organisation

Governmental organisations, which play the most important role in the comprehensive nuclear security regime in Hungary, are presented in the figure below and in more detail their role is explained in the previous Section of this Report.

Table 1. National organisation of bodies relevant for nuclear security in Hungary

Subject	Competent Authority	Co-authority
Licensing/Inspection	Hungarian Atomic Energy Authority supervised by the Ministry of National Developments	National Police Headquarters under Ministry of Interior (MI)
DBT assessment, establishment and update	Competent Authority: - Hungarian Atomic Energy Authority	Co-authority: - Constitutional Protection Office, Counter-Terrorist Centre and the National Police Headquarters under the MI and - Military National Security Service under Hungarian Defence Forces
Trustworthiness checks	Regional Competent Police Departments under MI	
Security Vetting	Constitutional Protection Office under MI	
Protection of sensitive information	Licensing authority for handling sensitive information: - National Security Authority of the Hungary (NSA) under the Ministry of Public Administration and Justice	
Classification of sensitive information related to the application of atomic energy	DG of HAEA	

In addition to the above mentioned for the more comprehensive picture of the structure of the State's physical protection regime several others has to be mentioned while of course following overview is not exhaustive and does not include all of the participants.

- **The Minister of Human Resources (MHR) and the Minister of Public Administration and Justice (MPAJ)** - through the National Public Health and Medical Officer Service (NPHMOS) - is the national Radiation Protection Authority. The latter is inter alia responsible for defining dose constraints, and emergency intervention levels.
- **The Minister of Rural Development** is inter alia responsible for defining the maximum quantity of radioactive materials that may be released to the atmosphere and into water bodies (discharge limits).

- The **National Environmental Radiation Monitoring System (NERMS)** currently consists of the following members representing different ministries, authorities and special installations as regulated by the Government Decree 275/2002 (XII.21):
  - Ministry of Human Resources (MHR)
  - Ministry of Rural Development (MRD)
  - Ministry of National Development (MND)
  - Ministry of Defence (MD)
  - Ministry of Interior (MI)
  - Hungarian Academy of Sciences
  - Hungarian Atomic Energy Authority (HAEA)
  - Nuclear Power Plant Paks (NPP Paks)
  - Public Limited Company for Radioactive Waste Management (PURAM)

  The activity of NERMS is governed by the NERMS Steering Committee and chaired by the Hungarian Atomic Energy Authority (HAEA). The NERMS Steering Committee approves the annual environmental sampling and measuring programme to be performed by the radiological monitoring networks belonging to the NERMS Members. NERMS Information Centre collects and processes the radiological data measured by the individual monitoring networks, and prepares the annual reports from the results.

- **Minister of Interior (MI) under which the National Directorate General for Disaster Management (NDGDM)** is operating as a central body for disaster management in Hungary; the Directorate General, among other duties and responsibilities (as for example – determining the professional requirements of prevention, rescue and disaster management; etc) is also directing and supervising the work of the subordinated organs, participates in the prevention and management of the expected consequences of nuclear accidents, natural or industrial disasters, as well as in the organisation of protection and planning at national level.

- **National Security Services** are divided into "National Civil Security Services" (**Information Office; Constitutional Protection Office and Specialised National Security Services),** and Military National Security Services. They are all budgetary agencies subject to the control of the Government. In addition to the role that some of these organisation have in security vetting procedures, some are participating in the process of determining the national threat assessment and in establishing national Design Basis Threat (Constitutional Protection Office, Military National Security Service). Besides these bodies the Counter-Terrorist Centre and the National Police Headquarters both under the MI also involved in the DBT assessment process.

- **National Tax and Customs Administration of Hungary (NTCA)** are operating portal monitors at boarders and airports and are involved if the illicit trafficking of nuclear or other radioactive material out of regulatory control occurs.

2.5. THREAT ASSESSMENT AND THE DBT

As provided in Section 3 of the *Government Decree 190/2011* the HAEA is responsible for the preparation of the national threat assessment for nuclear material, radioactive source, radioactive waste, interim store and final repository of radioactive wastes and nuclear facilities, so that the security regime covers all type of activities and facilities including nuclear facilities and repositories, as well as those using, storing or transporting nuclear or other radioactive materials. Such an assessment has to be periodically reviewed (once per year).

The national threat assessment serves as input for the establishment of national Design Basis Threat (and its subsequent reviews). For both, national threat assessment and national Design Basis Threat, the coordinating role is assigned to the HAEA in agreement with the National Police Headquarters (NPH), the Constitution Protection Office, the Military Security Office of the Hungarian Defence Forces and the Counter-Terrorist Centre. National DBT adopted in the form of HAEA's decision which is sent to the obligant and those organisations which participated in its preparation.

Government Decree 190/2011 provides also for a Specific DBTs for each nuclear facility (with the exemption of the Training Reactor), as well as for the various categories of nuclear and other radioactive materials being in use, storage or transport. Such facility and activity specific DBTs the HAEA had to establish (in the form of resolution) within 30 days after entering of *Government Decree 190/2011* into force. Such specific DBTs include the number of adversaries, their aim (sabotage or unauthorized removal), weapons, tools, vehicles, physical and tactical skills, and their insider support.

Good practice 03: By the legislation which clearly defines leadership role of the HAEA and taking into account the extent of those governmental organisation participating in the preparation of National Threat Assessment and Design Basis Threat as well as the unambiguous requirement for periodic reviewing, a wide range of obligants and in particular also the fact that the process extends to the adoption of so called specific DBTs clearly demonstrate that national system goes beyond the specific recommendations that serve as the internationally accepted standard in this field.

2.6. RISK BASED APPROACH

It is clear from *1996 Act* on Atomic Energy that the State has applied a risk based approach to the physical protection against the:

"Unauthorized removal during use, storage and transport of Category III nuclear materials and Category 2-5 radioactive sources and during processing, storage and transport of Category 2-3 radioactive waste."

Unauthorized removal and storage during use and storage of Category I and II nuclear materials and Category I radioactive sources, and during processing and storage of Category I radioactive waste

Unauthorized removal during transport of Category I and II nuclear material, Category I radioactive source and radioactive waste; and

Sabotage against systems, structures and components significant to radiological consequences."

2.6.1. Risk Management

Under the *1996 Act* the Parliament identified in Section 4 /(3)d of the Act that "the risk of occurrence of an extraordinary event shall be decreased, its occurrence shall be preventable, its consequences shall be eliminated in a planned manner, harmful effects of the potentially released radioactive material and ionizing radiation shall be decreased to the lowest reasonably achievable level."

The State has managed the risk by developing a DBT in conjunction with other appropriate organisations. From the national DBT they have then developed site specific DBTs for facilities and transport. The State has also identified "sabotage against nuclear facilities, nuclear materials, radioactive sources and radioactive wastes, as well as theft of such materials" as one way that harmful effects from ionizing radiations can be generated.

2.6.2. Graded approach

Under *1996 Act* on Atomic Energy in Section 31 the state has stated that "Physical protection shall be based on a graded approach, considering the actual level of threat, physical and chemical properties of the material, its suitability to make nuclear weapon and to commit a malevolent act, and the potential consequences corresponding to unauthorized removal and sabotage against nuclear and other radioactive materials and nuclear facilities".

The State has identified that the obligant shall realize the physical protection of the nuclear facility, interim storage and final repository of radioactive waste, such a way that ensure the effective protection against the design basis threat prescribed for the specific facility by regulatory decision. The state has further provided prescriptive objectives based on a defined physical protection levels. The State has defines 4 physical protection levels. Each security level identifies the graded protection measures needed.

The categorization table for radioactive wastes as detailed in Decree *190/201.*

Categorization of radioactive wastes

	A	B
1.	Radionuclide inventory (R)	Category
2.	$R \geq 1000$	1
3.	$10 \leq R < 1000$	2
4.	$1 \leq R < 10$	3
5.	$R < 1$	4

Where $R = \sum_i \frac{A_i}{D_i}$, while $R_{real} = R \times S_i$

A_i – activity of isotope i within the radioactive waste;
D_i – isotope specific normalizing factor for isotope i as defined in the KHEM decree;
S_i – factor considering the activity concentration of the radioactive waste, its dispersibility, the robustness of the radioactive waste package and its accessibility.

Basis: IAEA NSS No.14 Para 4.4:

A categorization system should be established that implements the graded approach by associating security levels (required degrees of protection) with specific types and quantities of radioactive material, thereby ensuring greater levels of protection for radioactive material for which a malicious act could result in higher consequences. The categorization system should take aggregation of radioactive material into account as appropriate. As a starting point, the categorization system should take into account international guidance such as the Code of Conduct on the Safety and Security of Radioactive Sources or the Regulations for the Safe Transport of Nuclear Material (TS-R-1).Good practices:

Good practice 04: The categorization of radioactive materials defined in the Decree is beyond the recommendations provided by the Code of Conduct on the Safety and Security of Radioactive Sources, the categorization addresses not only the 25 radionuclides listed in the Code of Conduct but all the radionuclides above the exemption activity limits and radioactive waste. Establishment by HAEA of categorization of Radioactive Waste for security purposes is based on clearly defined criteria. This allows the implementation of graded security requirements using the risked informed approach. This practice is commendable and it would be beneficial to share with other countries.

2.7. DEFENCE IN DEPTH

Per Section 31/(5) of *1977 Act* on armed security guard services, nature and field guard services "The physical protection system shall follow the protection-in-depth concept and shall provide multilevel and multi-method protection in accordance with the concept of balanced protection irrespective of the location, time and method of the action." The guidelines on Physical Protection (specifically guideline PP-7) discuss some of the details of the concept of protection in depth. This section identifies the physical protection areas and their relationship to one another.

2.8. SUSTAINING THE PHYSICAL PROTECTION REGIME

Security Culture

Under *Governmental Decree 190/2011*, "The obligant shall develop and maintain security culture necessary to ensure effective implementation of the physical protection system within the entire organisation and to ensure that each organisation, organisational unit and person manages the physical protection related activities with due importance."

In order to ensure an effective operation of the physical protection system the obligant shall provide entrance training and at least annual refreshing training in the area of physical protection for the persons holding permanent authorization to access. Security culture shall be covered as part of this training.

The State also requires that security culture be included as part of the obligant's annual evaluation of the performance of organisational and technical subsystems of the physical protection for the preceding year. The results are provided to the Hungarian Atomic Energy Agency as part of the annual report.

The HAEA has developed Guideline PP-6 on Security Culture which describes in detail the Roles and responsibilities of institutions, individuals, public and international community. This Guideline then goes on to describe some of the attributes of a good strong security culture.

Suggestion 03: Facilities consider providing regular reminders to employees about the importance of security. A simple method is displaying signage around the facility reminding employees about the importance of security and the importance of their role in security.

2.9. QUALITY ASSURANCE

The 1996 *Act* on Atomic Energy states in Section 11/(2) that "only such institutes, organisations and those entities according to Para c) of Section 685 of the Act on the Civil Code shall perform activities related to nuclear facilities, nuclear systems and equipment, which have appropriate quality management system." Furthermore it goes on to state in Section 31/(6) that "The licensee shall develop physical protection policy and quality management system and shall apply it to demonstrate that the requirements are complied with in relation to all activity important to physical protection."

Also in the Hungarian Atomic Energy Authority Guideline PP-11 (Preparation and submittal of physical protection license applications) the obligant must identify physical protection procedures and quality management data. In Guideline PP-6 it also states that "the security function and within that the physical protection matters require the same degree of rigor and control as the operation process. Therefore, standard quality management practices should be applied also in this field"

2.10. CONFIDENTIALITY

Information security and protecting the confidentiality of information associated with nuclear security is a fundamental principle for nuclear security. The State has the ultimate responsibility for establishing the requirements for confidentiality and the protection of information and computing systems related to physical protection, nuclear safety, and nuclear material accountancy and control. This includes information stored on electronic media and computing systems. Likewise the State maintains sensitive information related to the security, storage, and management of nuclear and radiological materials that requires protection.

Hungary has a national information security policy 2009 *Act* on the Protection of Classified Information that addresses *classification of information.* The National Security Authority (NSA) is responsible for the official supervision of the protection of classified information, the licensing and supervision of the management of classified information, and the fulfilment of national industrial security official responsibilities.

Act CLV defines the following terms and concepts related to information security*:*

- *national classified information:* information within the scope of public interest to be protected by classification, fulfilling the formal requirements of regulations issued under this Act and marked for classification through this Act, for which – irrespective of its form – the information classifier defined through the classification process that

within the term of validity, any kind of disclosure, unauthorised access, amendment or usage, providing access for unauthorised persons or blocking the access of authorised persons can directly harm or jeopardise (hereinafter jointly: damage) public interests to be protected by classification and will limit its disclosure and access to its contents through classification;

- *user licence*: a written authorisation issued for the person entitled to use classified information by the official authorised to issue such licences for the fulfilment of state or public responsibilities with specific definition of the right of disposal over the classified information;
- *access permission*: an authorisation issued in written form by the information classifier, displaying personal identification data of the authorised person, concerning the definition the right of disposal of national classified information for the purpose of accessing national classified information;
- *confidentiality declaration*: a declaration of the person using or having access to classified information on being aware of the rules and regulations for the protection of classified information and their acknowledgement of confidentiality obligations;
- *personal security certificate*: a certificate to define the highest level of classified information a natural person can access with a user licence within its term of validity;
- *economic entities:* as enlisted in subsection 685 c) of Act IV of 1959 on the Civil Code,;
- *site security certificate:* the certificate to determine the highest level of classified information the economic entity is suitable to manage;

The handling of classified information is limited, with exception, to those who have obtained a licence issued by the National Security Authority

Classified information shall be handled solely on the basis of the licence issued by the National Security Authority and access to classified information shall exclusively be granted to individuals (with certain exemptions per the Act) with personal security certificate and confidentiality declaration, with the rights of disposal defined in the user licence. [Chap 4, Section 10, par 1 and 2]. The NSA also has response responsibilities should a security incident occur involving classified information or systems.

Act CLV further defines a graded approach to information protection based on four information categories based on the potential damage that disclosure within the term of validity, unauthorised obtainment, modification or use of the piece of information, or granting an unauthorised person access or blocking an authorised person's access to such information could cause.

These levels are

- Top Secret,
- Secret,

- Confidential, and
- Restricted.

Annex 1 of Act CLV of 2009, included as an attachment to this report, details the qualifying requirements for each level.

Act CLV further specifies in Chapter IV "Amending Regulations" basis for the punishment for violation of information protection requirements through amendments to the *Criminal Code*.

While the requirements for government activities originating and handling classified information are clear, it is less clear as to the applicability of this legislation and processes specific to nuclear and other radioactive material facilities that are possessing nuclear security sensitive information.

Section 16/(4) of the *Act CLV* specifies:

(4) Classified information of 'Confidential' or higher classification level can exclusively be referred to economic entities with valid site security certificate.

Organisations handling classified information must obtain a *site certificate*. Different licenses are required for hard copy materials and information stored in electronic systems. A *user license* is additionally required for an individual to be allowed to handle classified information. Act CLV provides information detailing the requirements for obtaining site security certificate. The NSA is the granting authority for such licenses. In cases where the organisation does not have a *site certificate*, but does have individuals that have user licenses, the HAEA provides security facility for use and storage of the information.

The HAEA is the classifying authority for sensitive nuclear security information from licensees. Nuclear facilities submit site security plans to HAEA with a recommended security classification level (i.e. Top Secret, Secret, Confidential, and Restricted) under the national classification scheme, with a justification for the recommended classification. The HAEA Classification Officer reviews the proposal and classifies the security plan submitted by the licensee. The facility must have a *site certificate* and the appropriate individuals' *user licenses*. Specific information security requirements are specified in national legislation.

Licensees which are not required to classify such documentation under the national classification framework must specifically address the information security of the site security plan and associated sensitive nuclear security information within the site security plan. The HAEA reviews and approves these requirements as part of the licensing process.

2.11. SUSTAINABILITY

It is clear that the atomic energy oversight organisation (HAEA) which is a government office will be sustained by a fee to be paid through an agreement with the minister responsible for taxation.

Even though there is no specific law, decree or regulation for a sustainability program it appear that the laws, decrees and regulations which are in place address the components that the state and the obligants must have to sustain a physical protection regime.

2.12. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENT

The state requires "In order to prevent the occurrence of a nuclear emergency situation, to respond to or mitigate the consequences of an event that has occurred, as well as to restore the prescribed regular circumstances, the user of atomic energy is obliged to: elaborate an emergency preparedness and response plan and have it approved by the competent authorities; establish the personal, material and organisational conditions for efficient emergency response and to regularly verify the meeting of these conditions from time to time; ensure the conditions required for external assistance necessary for emergency response (nature, extent and method of such assistance) in agreement with the competent authorities and organisations."

Section 18/(2) of the *Government Decree 190/2011* states "The obligant as part of the physical protection plan, shall prepare a contingency plan, which specifies the scope of possible events, including also the events that may cause inappropriate operation of the physical protection system, as well as the procedure of necessary measures and interventions.

Sections 18 goes on to say that the "obligant shall harmonize the management of nuclear and non-nuclear emergencies with the operation of the physical protection system.

Section 31/(7) of *1996 Act* states the atomic energy oversight organisations, the police and the licensee shall develop plans and adequately exercise the implementation of the plans to be able to adequately respond to unauthorized removal of and sabotage against nuclear materials.

4. TRANSPORT REVIEW

The IPPAS team have visited a number of facilities where Nuclear Material (NM) and Radioactive Materials (RAM) are located, including several locations where high activity radioactive sources are used for different applications. This transport section addresses the activities associated with the transport of NM and RAM, based on the aforementioned facilities involved in transport that were visited as part of the review process and following discussions with the HAEA. The HAEA guideline PP15 provides specific and well defined guidelines for the transport of NM and RAM.

Two companies are licensed carriers to transport NM while several companies are licensed to transport RAM. The requirements on physical protection for the transport of NM are based on the categorisation table of NM in CPPNM and for the categorisation of RAM, it is based on the code of conduct. The graded approach for the physical protection of NM and RAM during transport is applied according to the categorisation of the NM or RAM, applying the appropriate Security Level A, B C or D as laid down by the HAEA. The appropriate physical protection measures for transporting NM or RAM should then be implemented based on the Security Level of the material. Based on the national DBT specific requirements are defined and a prescriptive approach concerning the physical protection requirements is applied to the licensed companies transporting NM and RAM.

A regulatory licence is required to transport NM and RAM. The licence is valid for five years, except for the transport of NM and RAM requiring Level A or B physical protection, in which the licence is only valid for the specific transport. During the transport of NM and RAM it was ascertained that measures are undertaken to ensure that NM and RAM is protected against unauthorised removal, since it could have significant consequences if dispersed or used otherwise for a malicious purpose. It was established that when required comprehensive Physical Protection Plans are submitted to the HAEA for authorisation of the physical protection system to be applied during the transport of NM and RAM. The impression from the IPPAS Team is that the sampling of these activities represents the majority of transport operations and the licensed shippers within Hungary. During the IPPAS mission, the Team did not observe any transport movements. The conveyances used for transporting NM and RAM by the licensed carriers in Hungary are by rail, road and air.

The Physical Protection Plans for the transport of NM and RAM detail the deterrence, detection and delay measures and implementation of response actions to be applied in the event of attacks against the shipment. Contingency plans are prepared for the transport of NM and RAM detailing the procedures and actions to be implemented in the event of potentially expected, but credible threats or attacks against the shipment. In addition to incidents occurring during the transport of NM and RAM the contingency plans also cover accidents and technical breakdowns of the transport conveyances.

In addition to the review of the transport of NM following the guidelines in the INFCIRC/225/Rev 5, the IPPAS Team were requested to review the transport activities of RAM according to the recommendations contained in the IAEA NSS No 14 entitled, "Nuclear Security Recommendations on Radioactive Materials and Associated Facilities". As detailed in the NSS No 14, when a facility contains NM and RAM, the protection requirements for both should be considered and implemented in a consistent and non-conflicting manner in order to achieve an adequate level of security. Consequently, during the review the physical security protection for the transport of both NM and RAM was taken into consideration. Further, when evaluating the physical protection measures for the transport of RAM, the implementing guide IAEA NSS No 9 entitled, "Security in the Transport of Radioactive Material' was used as a base for suggestion.

The IPPAS team concluded based on the information available that the physical protection system appeared to be effective and well maintained. The findings identified during the IPPAS mission of the requirements for the measures to be applied during the transport of NM and RAM are detailed below:

4.1. Threat and Target Identification

The physical protection measures applied during the transport of NM and RAM are based on a graded approach taking into account the current evaluation of the threat and the nature of the material to be transported.

4.2. Allocation of Responsibilities

The responsibility for the implementation of physical protection of NM and RAM rests with the operators and licensed carriers who are the holders of the relevant licences.

4.3. Transport Security Planning and Implementation

A regulatory licence is required to transport NM and RAM. The licence is valid for five years, except for the transport requiring Level A or B physical protection, when the licence is only valid for the specific transport. In accordance with the Government decree 190/2011, a physical protection plan is required for the transport of NM and RAM. The transport physical protection plan shall include a description of the material to be transported, the name, position and contact details of the person responsible for physical protection during the transport and a description of the transport means and vehicle, together with a detailed drawing of the transport vehicle.

4.4. Security Training and Qualifications

The competent authority and the operators advised that there is a training programme for security personnel involved in the transport of NM and RAM, which includes response to nuclear security events as specified in the transport security plan.

4.5. Security Culture

Security training for the operators, carriers and the response forces includes a security awareness programme and that all those involved in the transport of NM and RAM work together to promote and maintain a security culture.

4.6. Quality Assurance

A lessons learned programme exists to identify and correct quality issues identified within the physical protection system. Dependant on the occurrence, if it is required the HAEA will amend the guidance on the 'Preparation of the physical protection plan required for the transport of nuclear and other radioactive materials', in order to prevent a recurrence.

4.7. Confidentiality and Information Protection

The physical protection plan for the transport is considered a sensitive document. The storage place and method of storage of the transport physical protection plan is detailed in the transport physical protection plan together with the names and positions of those having access to it.

Transport guidance document PP15 details the handling requirements for this information, but the actual storage and handling processes for this information could not be confirmed during the review.

4.8. Sustainability Programme

The Team recognised that a systematic approach existed to ensure the continuous reliability of personnel and operating procedures for the transport of NM and RAM.

4.9. Evaluation Including Performance Testing

Exercises are conducted to evaluate the performance capabilities of the physical protection system for the transport of NM and RAM.

4.10. Interface with Safety and Nuclear Material Accountancy and Control

The site licence holder assesses and manages the physical protection interface with safety and NM and RAM accountancy and control activities in a manner that ensures they are mutually supportive and complement each other. The receiver of NM and RAM checks the integrity of the packages, locks and seals when used and accepts the shipment immediately upon arrival.

4.11. Trustworthiness

Necessary trustworthiness checks are conducted for personnel and security staff involved in the transport of NM and RAM.

4.12. Reporting

Arrangements and procedures are in place for timely reporting of all events relevant to the security of the transport of NM and RAM.

DETECTION

4.13. Access Control Including Searching

Detailed searches of conveyances are conducted to ensure that nothing has been tampered with and that nothing has been affixed to the package or conveyance that might compromise the security of the assignment. Additionally access control is implemented to deny unauthorised access of persons or the introduction of prohibited items into the vicinity of the packages and conveyance. It was ascertained that the Hungarian National Police have the responsibility for ensuring that personnel are trained to conduct searches of the conveyances use for transporting NM and RAM.

4.14. Intrusion Detection

Required intrusion detection equipment is installed for the transport of NM and RAM.

4.15. Transport Control Centre

A Transport Control Centre is manned when transporting Category II and III NM and Category 1 RAM. The Transport Control Centre is set up in a designated room within either the facility the material is being transported from or where the shipment is being transported to. The two main functions of the Transport Control Centre are to act as a Communications Centre and the centre for tracking the transport. The Transport Control Centre also becomes the decision making centre in the event of any incidents occurring whilst transporting the NM or RAM. The Transport Control Centre is staffed by technical experts and the required decision makers and they are all confirmed as being trustworthy. The operation of the Transport Control Centre is detailed in the transport physical protection plan.

The Transport Control Centre tracks the movement by tracking the driver of the vehicle who is given a GPS tracker.

Suggestion 23: When using GPS tracking, make the GPS tracker integral to the vehicle and not the driver.

4.16. Locks, Keys and Seals

Where practicable, locks and seals are applied to conveyances and checks are made before dispatch and by the receiver upon delivery. The use of locks and seals is not consistent between the different carriers/shippers.

During the visit and review of two shipping vehicles, the Team observed that the carrier did not provide two barriers to protect radioactive sources.

The use of a cage is a requirement by the regulation, with the exception when the package is too large for a cage.

Suggestion 24: When a cage is not in use as a second barrier for transport of Category 1 and 2 RAM, alternative means for a secondary barrier could be applied (e.g. such as a chain, or padlock) for, so that the package is attached to the vehicle.

DELAY

4.17. Resistance to Forcible Attack

It was identified that for the transport of Level B NM and RAM, the vehicle or the storage plate cabinet doors shall exhibit resistance against an intruder equipped with special tools for a minimum of 10 minutes. Suitable physical protection measures are in place to provide sufficient delay in the conveyance or freight container in order that the Security Guards and response forces have time for an appropriate response.

4.18. Guards and Response Forces

PP15 guidelines establish that for B-Level transport movements of NM and RAM, response by the police shall be affected within 10 minutes. Additionally, it was ascertained that an on Site response force is a preferred option. During the transport of NM and RAM the police are located at a 'special place' and that the police response force would take 10-15 minutes to respond. The Transport Security Contingency Plans were assessed as not being specific as to where the response force is located in order to arrive in time to prevent the unauthorised removal of NM and RAM and there was a disparity in the time taken to for the police response force to respond.

Suggestion 25: Conduct an exercise for NM and RAM transport to verify police force response times during a security event.

4.19. Communications

The transport of Level B, C and D NM and RAM, reliable mobile communication shall be provided. During transport movements of Level B material, the escort team shall establish periodic communication with the driver of the vehicle, the Site licensee, the consignee, the local authorities and the response forces. The driver uses a cell phone to communicate with the escort and the police.

4.20. Contingency Plans Including Exercises

Contingency plans exist in order to respond to a security incident involving the transport of NM and RAM. In addition to addressing incidents occurring during the transport of NM and RAM, the contingency plans also cover accidents and technical breakdowns of the transport conveyances. It was reported that the response force is familiar with the transport operations and that the contingency plans are exercised.

4.21. Equipment

The Team identified that suitable equipment is available for the Security Guards and response force to properly perform their duties during the transport of NM and RAM.

4.22. Transport Vehicles - Radioactive Materials

Specific vehicles are used for the transportation of radioactive material (Category 1-5) throughout the country. The vehicles are equipped with security features such as detection sensor on the rear door of the cargo space, video camera inside the cargo monitored by the driver, and additional security lock on the rear door. During the visit the team discussed the

transport of Category 1 and 2 radioactive materials only. The IPPAS team has identified some suggestions based on the IAEA implementing guide NSS No 9 Security in the Transport of Radioactive Material.

Detection

Seals or other tamper detection devices are not consistently fixed to the external side of the doors to detect unauthorised access to the package.

Suggestion 26: Consider using seals or anti tamper device fitted to the external cargo doors and provide procedures for the use of the seals and anti tamper device.

A vehicle pre-inspection check does not follow specific procedures and is not documented by an individual independent of the transport operation.

Suggestion 27: Consider formalizing procedures to conduct pre-inspections of conveyance prior to transport. Consider conducting pre-inspection vehicle checks by an independent individual not involved in the specific transport operation. This individual could be part of the same company, such as quality assurance.

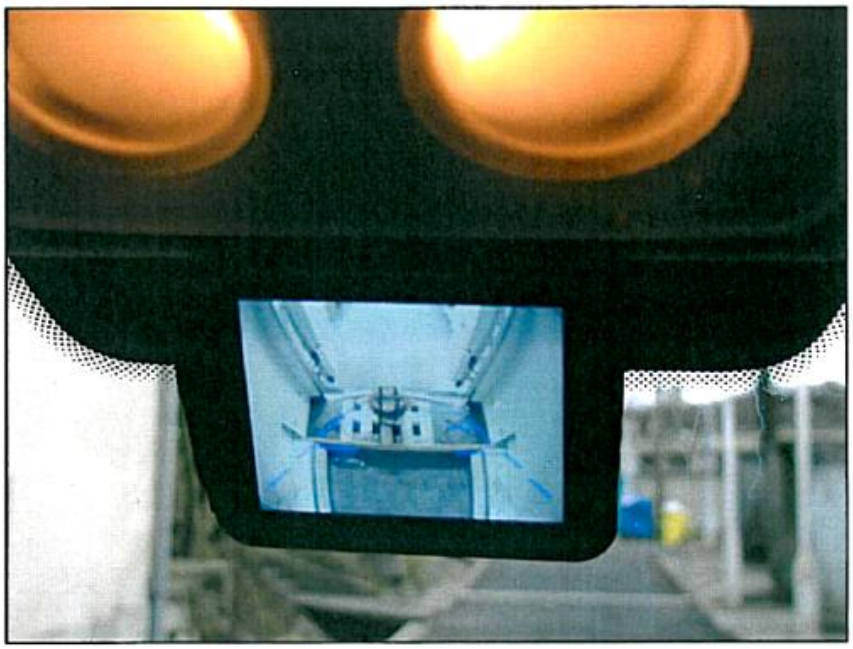

Figure 18. Video system to monitor the cargo

Response

The team observed that the vehicle used a mobile GPS tracking device which could be removed and placed in another vehicle.

5. SECURITY OF RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES

In Hungary there are 7000 sealed sources of radioactive materials above exemption level, owned by 380 users. Of these 262 are Category 1, 1567 are Category 2, 367 Category 3, 1068 Category 4 and 3765 are Category 5. Associated facilities using radioactive material are the sealed source producers of Co-60 and Ir-192, irradiation facilities (blood, agricultural, medical), teletherapy units in hospitals, gamma knifes, industrial gamma radiography, high/medium level dose brachytherapy and industrial gauges.

Besides nuclear facilities there are about 30 other users that use or store nuclear materials, e.g. research, calibration.

The primary facilities dealing with radioactive materials in Hungary are the following:

- **Central Isotope Storage, Budapest.** The storage is located on the site of the Budapest Research Reactor. The Central Isotope Storage is used for the temporary storage of disused radioactive sources (including nuclear materials) of all the research institutes on the site.

- **Minewater Treatment Plant of the Mecsek Öko Zrt., Kővágószőlős (Pécs).** While the Headquarters of the Mecsek Öko Zrt. is located in the city of Pécs, its Minewater Treatment Plant operates at Kővágószőlős. In order to meet the health and environmental authority requirements, the uranium content of the surface and subsurface water contaminated by the former mining and milling activities is removed in the Minewater Treatment Plant to protect the two water reservoirs located in the area. During a continuous process the uranium is concentrated in the form of uranium oxide ("yellow cake") and is exported (~2-3 tons/year).

- **Radioactive Waste Treatment and Disposal Facility.** The Radioactive Waste Treatment and Disposal Facility (RWTDF) at Püspökszilágy site is operated by Public Limited Company for Radioactive Waste Management (PURAM). It receives 5 to 15 m^3 of low and intermediate level waste annually from smaller radioactive waste producers (hospitals, laboratories and industrial companies). Several thousand used radiation source are stored there at the facility.

- **Locations outside facilities with small amount of nuclear materials.** There are 39 licensed locations outside facilities (LOFs) having small amount of nuclear material. The "small users" of nuclear sources are usually universities (Debrecen, Budapest,

Veszprém), research institutes (ATOMKI, VEIKI, OSSKI) and other companies which use nuclear material for industrial applications.

5.1. Security Approach

The national approach for the application of security levels to radioactive materials sources is based on a prescriptive and graded approach. The required security levels are listed below and are compared to the levels specified in the implementing guide NSS No11.

Table 2. Mapping of Security Levels for Radioactive Materials

Code of Conduct Source Category	Security Level Govt. decree No. 190/2011		Security Level IAEA – NSS No. 11	Code of Conduct Source Category
1	B	→	A	1
2	C	→	B	2
3	C	→	C	3
4	D		Prudent Management Practice	4
5	D		Prudent Management Practice	5

Note that the Security Level B according to Decree 190/2011 specifies similar measures of security as Security Level A according to IAEA NSS No. 11 and similarly Security Level C in Decree 190/2011 specifies similar measures of security as NSS No. 11 Security Level B. Therefore in Hungary, Category 3 sources are protected to the equivalent of NSS No. 11 Level B security. Furthermore, specific measures (level D in Hungary) are required for Category 4 & 5 radioactive materials whereas only prudent management practices are specified in NSS-11.

The remainder of this section refers to the security levels applied in Hungary.

6. COMPUTER SECURITY REVIEW

Computer based systems are used extensively in physical protection, nuclear safety, and nuclear material accountancy and control systems at nuclear facilities. The duration of this IPPAS mission precluded an in depth review of computer policy and programme records for the competent authority and the selected nuclear facilities, therefore the review focused on discussions with the respective organisational computer security experts and a review of the legal basis for computer security at these facilities.

The review consisted of discussions with representatives:

- Hungarian Atomic Energy Authority
- National Security Authority
- Paks NPP and its parent company MVM
- Interim Spent Fuel Storage Facility

6.1. State Level Review

The state level review for computer security associated with nuclear and other radioactive material, facilities and associated operations consisted of briefings and discussions with by Hungarian Atomic Energy Authority and the National Security Authority, and a review of relevant legislative acts.

6.1.1. Legal Framework

The *1996 Act* on Atomic Energy (Atomic Act) establishes the rules for use of atomic energy. The nuclear safety requirements for nuclear facilities and the corresponding regulatory activities are determined by the Govt. Decree 118/2011 (VII.11.) Korm. and its Annex, the Nuclear Safety Code (NSC). The requirements for physical protection in the field of atomic energy are described by the Govt. Decree 190/2011 (IX.19) Korm.

Computer security requirements are not addressed by a specific separate decree, but are extracted from multiple paragraphs taken from each decree. The following relevant paragraphs of the decrees were noted:

6.1.2. Governmental Decree 190/2011 about Requirements of Security of Atomic Energy

Relevant paragraphs of Decree 190/2011 are paraphrased below:

- In the nuclear installations, in nuclear or radiating material storage or radiation source facilities the defence in depth principle should be applied, and security zones should be established on the controlled area of the facility. (14. § (1))

- The allocation of I&C and computer systems and components including the data transmission systems and related cabling should follow the physical boundaries of security zones. (20. § (1))
- The data transmission from the highest security level safety zones may have only one direction. The one direction data transfer should be assured on physical principles, and should not be provided only with computer protocol and programmed means.(20. § (2))
- The credibility of on-line input data and the data readings from data storage hardware should be checked, including that data storage which is necessary for restoration. (20. § (3))

6.1.3. Govt. Decree 118/2011 Nuclear Safety Code requirements related to Cyber Security

Relevant paragraphs of Decree 118/2011 are paraphrased below:

- The systems and instruments that provide functions to operate executors of protective and safety systems, as well as collection and display functions of data of nuclear safety importance which aid the decision-making of operational personnel shall be protected against external information technological influence which may theoretically enable the modification or disabling of a safety function. (NSC 3.4.5.3700)
- The systems and instruments that provide functions to operate executors of protective and safety systems, as well as collection and display functions of data of nuclear safety importance which aid the decision-making of operational personnel shall be so established that data flow is only possible from the inside to the outside. (NSC 3.4.5.3800)
- The safety zones shall be established in correspondence with the opportunities of physical access to the systems and instruments, including the arrangement of information technology data transfer instruments and data cables. (NSC 3.4.5.3900)
- The necessary administrative system and the safety protocol of the associated internal procedure and accesses shall be developed:
    - for the performance of maintenance necessary in the systems,
    - for the necessary modification of the digital systems,
    - for the detected program and data errors, and
    - for monitoring the inward and outward transport of data carriers. (NSC 3.4.5.4000)

6.1.4. Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies

The provisions of this Act are applicable to the protection of the electronic information systems for government entities, but also include

- those performing data management for such agencies,
- the data processors of statutorily defined public records within the scope of national data assets,
- system elements designated by law as European vital system elements or national vital system elements.

The vital system elements refer to information system and would not be applicable to the breadth of electronic systems at a nuclear facility such as a nuclear power plant.

Each organisation under the purview of this act shall classify their electronic information systems using a scale from 1 to 5, depending on the confidentiality, integrity and availability risks related with the electronic information system or the data managed therein, where a higher rating shall require stricter protection rules.

Section 11 of the Act details the obligations of organisations with respect to electronic information system protection. These are:

(1) The head of organisation shall arrange for electronic information system protection by:

- ensuring compliance with the legal requirements for the security class applicable to the electronic information system,
- ensuring compliance with the legal requirements for the security level applicable to the organisation,
- appointing or entrusting a person in charge of electronic information system security in accordance with the requirements of the security class of the electronic information system and the organisation's security level; such person may be identical with the security manager defined in Act CLV of 2009 on classified information protection,
- issuing the information security policy applicable to the organisation's electronic information systems,
- determining the information security strategy applicable to the organisation's electronic information systems,
- making rules for the persons in charge of, and the tasks related to, the protection of the organisation's electronic information systems, for the required powers and users, and by issuing an information security regulation,
- ensuring training courses on the protection tasks and responsibilities related to electronic information systems, and maintaining his or her own information security skills and those of other staff,
- conducting regular security risk assessments, inspections and audits to be satISFSed that the organisation's electronic information system security complies with the relevant laws and risks,
- ensuring the traceability of incidents in the electronic information system,

- using all necessary and available resources to arrange for a rapid and efficient response to any security incident which has occurred and for the subsequent management of such security incident,
- ensuring compliance with the provisions of this Act as contractual obligations when using a third party to create, operate, audit, maintain or repair the electronic information system,
- ensuring compliance with the provisions of this Act as contractual obligations when the organisation uses a third party for data management or data processing activities,
- being responsible for informing all affected parties about security incidents and potential threats in a timely manner,
- taking any other action required for electronic information system protection.

6.1.5. Critical Infrastructure

In addition to the Act for the *Electronic Information Security of Central and Local Government Agencies*, an Act has recently been approved on computer security requirements for Hungarian critical infrastructure. This document was not available for viewing.

After discussion with HAEA and NSA in regards to this document, it was not clear if the act was applicable to nuclear facilities such as nuclear power plants. This issue relates to the definition of critical infrastructure by the European Union.

6.1.6. Cyber Security Regulation

In Hungary no Act or Decree specifically addresses the computer security of nuclear, other radioactive material facilities and associated activities. Parallel exists in national law, but the applicability is not clear. Likewise, components can be drawn from nuclear safety and physical protection laws, but precise and complete legislation does not exists related to computer security obligations for computer systems associated with nuclear safety, security and material accountancy and control.

The HAEA has developed a draft guideline, "PP-18 Guideline: Protection requirements for computer systems", which is significant, but the competent authority and licensee could benefit from a stronger legal basis.

Additionally, the HAEA does not have a current oversight structure or exercise structure to perform assurance activities associated with cyber-security as a component of nuclear security at its licensed nuclear facilities.

Basis: NSS 20, Essential Element 12: Sustaining A Nuclear Security Regime

3.12. A nuclear security regime ensures that each competent authority and authorized person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:

(h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber-security, at all times.

Basis: INFCIRC/225/Rev. 5; Para 4.10 /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.

Suggestion 51: Develop requirements for cyber-security programme implementation to address the protection of computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control associated with regulated nuclear facilities. The Act L of 2013 Act on the Electronic Information Security provides a framework that might be used for such legislation.

Suggestion 52: Develop a computer security oversight programme for regulated nuclear, other radioactive material facilities, and associated activities.

Good Practise 13: Hungary has implemented a cross-organisational cyber security working group consisting of government, competent authorities, and licensees collaboratively work together to discuss the implementation of cyber security at nuclear facilities. This group has worked together to develop "PP-18 Guideline: Protection requirements for computer systems".

6.1.7. Cyber Threat Characterization and Reporting

Given today's environment and known threat tactics, it is important to consider adversarial capabilities and scenarios related to a cyber attack on nuclear, other radioactive material, and associated facilities.

Basis: INFCIRC/225/Rev. 5; Para 3.34:

The appropriate State authorities, using various credible information sources, should define the threat and associated capabilities in the form of a threat assessment and, if appropriate, a design basis threat. A design basis threat is developed from an evaluation by the State of the threat of unauthorized removal and of sabotage.

Recommendation 09: The Competent Authority(ies) and licensees should integrate adversarial cyber capabilities and cyber attack scenarios as a threat analysis component for nuclear, other radioactive material, and associated facilities.

In April 2013, the State has approved legislation that will establish a national cyber security defence strategy. This law based on the strategy will take effect in July 2013. The law directs the creation of the

Government Incident Management Centre (GovCERT) as an incident response organisation to respond government cyber incidents at government facilities, but also to coordinates the operational activities of Sectoral Incident Management Centres, thereby participating in the sharing of information.

This structure is to replace the now defunct National Network Protection Centre (PTA CERT-Hungary).

Given this new organisation, the response procedures and communication protocols for the State to respond and to provide assistance to a cyber attack occurring at a nuclear facility, for example on a process control system of a nuclear power unit, have not yet been precisely defined.

6.1.8. Computer Security Guide

The objective of the "PP-18 Guideline: Protection requirements for computer systems" is to provide that such protection measures and a protection plan incorporating such measures are developed, which ensure at an acceptable level the designed operation mode of programmable systems and components and the availability, integrity and confidentiality of the data processed, stored or forwarded in programmable systems and components which are:

- connected to system components fulfilling nuclear safety function, or
- connected to system components fulfilling physical protection function, or
- connected to system components important from the aspect of operation of the facility.

The Guide provides a background and basis for recommended practices in computer security.

This document was reviewed by the Team and the following suggestions are provided.

Suggestion 53: Update the draft "PP-18 Guideline: Protection requirements for computer systems" to include formal processes for the communication of cyber threat information between the Government Incident Management Centre, Sectoral Incident Management Centres, the National Security Office, and licensees.

Suggestion 54: Update the draft "PP-18 Guideline: Protection requirements for computer systems" to include incident response procedures for cyber events at licensed facilities. The procedure should address both internal and external response responsibilities, mitigation plans, and reporting requirements to the Competent Authority and respective national organisations (e.g. Government Incident Management Centre, Sectoral Incident Management Centres, and the National Security Office). It is understood that new response structures will be adopted July 1, 2013 with the enactment of the new law.

Good Practise 14: Hungary has implemented a cross-organisational cyber security working group consisting of government, competent authorities, and licensees collaboratively work together to discuss the implementation of cyber security at nuclear facilities.

7. ACKNOWLEDGEMENTS

Members of the IPPAS team wish to express their appreciation to the staff of the HAEA and of other authorities who contributed to the success of the IPPAS mission. The IPPAS team was privileged to meet with the many professionals who freely offered their expertise and time and appreciates the time they spent patiently answering numerous questions.

The HAEA provided valuable support to the IPPAS mission members. The comprehensive advance information considerably assisted the IPPAS mission. Key members of the facilities visited were most helpful throughout the team's tour by providing insight into facility operation, and the organization and implementation of physical protection measures and emergency response.