COUNCIL OF THE EUROPEAN UNION

Brussels, 31 May 2012

10616/12

AHGNS 20
ATO 84

NOTE

from :	General Secretariat of the Council
to :	Delegations
Subject	Ad Hoc Group on Nuclear Security - final report

Delegations will find attached the final report of the AHGNS as agreed on 24 May.

Report of the Ad hoc Group on Nuclear Security

Table of Contents

1. ESTABLISHMENT OF THE AD HOC GROUP ON NUCLEAR SECURITY (AHGNS)

After the Fukushima disaster, the European Council of 25 March 2011 decided that "the safety of all EU nuclear power plants (NPPs) should be reviewed, on the basis of a comprehensive and transparent risk and safety assessment ("stress tests")[1].

In May 2011 the European Nuclear Safety Regulators Group (ENSREG) and the Commission agreed that a two-track process should be put in place to cover the safety and the security. The scope and modalities of the safety track were agreed and the tests officially started on 1 June 2011. The preliminary outcome of this work was reported to the European Council of 9 December 2011.

To take forward the security track a new Presidency-chaired Ad Hoc Group on Nuclear Security (AHGNS) was created on 21 July 2011 on the basis of the COREPER decision and a mandate (document 13111/11 + ADD 1 RESTREINT UE). The group should deal with security of the NPPs in EU in relation to theft, sabotage, unauthorised access, unauthorised movement of nuclear material or other malicious act.

In contrast to the safety track of the "stress tests" , the work of AHGNS on the security track has not dealt with specific NPPs nor has it discussed Member States' special characteristics but has concentrated - according to the mandate – on methods for evaluating, taking preventive measures and protecting NPPs. The goal of the work of AHGNS has been to identify and share good practices and consider possible ways to improve general security principles based on the nuclear security recommendations of the International Atomic Energy Agency (IAEA).

The preliminary outcome of the work in AHGNS was reported in an interim rapport (document 17061/11+ COR 1) submitted to the European Council of 9 December 2011. This final report does not contain classified information.

2. WORK PROGRAM AND WORKING METHODS

2.1. The Period July – December 2011

During the Polish Presidency the AHGNS had five meetings. Bearing in mind the tasks indicated in its mandate, the AHGNS organised its work along three activities:

[1] EUCO 10/1/11 REV 1.

- Collecting information
- Processing information
- Preparing the interim report in view of the December 2011 European Council

As the key instrument to fulfil the first above mentioned activity the Polish Presidency prepared a questionnaire[1] that was circulated on 6 September 2011 and elicited replies covering almost all Member States. To a large extent these replies addressed the questionnaire in a comprehensive manner.

One of the four meetings was devoted to analysis of Member States' replies to the questionnaire, especially the elements that appeared to be shared in substance by most replies to the questionnaire and from which a series of specific good practices, currently implemented, could be identified. The last three meetings in turn were dedicated to drawing up the interim report. The resulting 32 good practices were grouped under the five headings:

A National legal and regulatory framework,
B National security framework,
C Design Basis Threat,
D Nuclear security culture
E Contingency planning

The interim report (17061/11 + COR 1 LIMITE) included 32 good practices which are found in Annex I.

With regard to the terrorism context indicated in the AHGNS mandate, most AHGNS meetings were attended by representatives of the EU Counter Terrorism Coordinator`s Office. Furthermore, a representative from ENSREG presented the working plan for the "stress tests" (safety track) carried out on the NPPs in EU.

2.2. The Period January – June 2012

During the Danish Presidency the Group met six times. Five themes were selected for more detailed analysis:

[1] 13773/11 RESTREINT UE/EU RESTRICED.

- Computer Security/Cyber Security
- IAEA's International Physical Protection Advisory Service (IPPAS) Missions
- Intentional Aircraft Crash
- Nuclear Emergency Planning: Synergies and consistency between Safety and Security
- Exercises and Training

Experts from one or more Member States introduced the theme by presentations, and the theme was subsequently discussed in the Group. Altogether 10 Member States have contributed with 14 presentations on their national experience within the selected themes. IAEA participated with a presentation at the first meeting when the IPPAS theme was discussed.
The five themes are presented in section 5.
Croatia, as an acceding Member State, joined the AHGNS in January with observer status.
The chair of European Nuclear Security Regulators Association (ENSRA) was invited as an observer to the last four meetings of AHGNS and gave a presentation on the work of ENSRA.
After decision by the AHGNS the Danish Presidency invited nuclear security experts from EU's neighbouring countries to a specific meeting in Brussels on 11 April 2012, where the preliminary work of AHGNS was presented and views on NPP security were exchanged (see section 6).

In the mandate for AHGNS, it is stated that AHGNS and ENSREG shall inform each other of any recommendations resulting from their respective proceedings in connection with aspects of nuclear security. However, the "stress tests" work (safety track) carried out by ENSREG deals with specific NPPs, while the work of AHGNS on the security track deals with methods for evaluating, taking preventive measures and protecting NPPs. The value of coordination between these two different ways of working has therefore been limited.

Furthermore, the work plan of ENSREG means that the results from the "stress tests" work have not been available before 25 April 2012, which was shortly before AHGNS had to complete its work.

AHGNS has on several occasions received information about the progress of the work on the "stress tests". In November 2011 an ENSREG representative made a presentation about the planned work in ENSREG, and the Danish Chair of AHGNS had a meeting with the ENSREG Chair on 11 April 2012, where the AHGNS Chair presented the preliminary results from the group, including the selected themes (see Section 5).

3. NUCLEAR SECURITY IN AN INTERNATIONAL CONTEXT

3.1. Nuclear security: What it is about

In some languages only one word applies both to safety and security to designate the prevention of hazards and the prevention of malicious acts and the term "physical protection" was introduced to cover what is now called nuclear security. In other languages depending on the field of activity safety means security and security means safety. In this document, on the basis of the international work carried out by the IAEA, nuclear security refers to:

"The prevention and detection of and response to, theft, sabotage, unauthorised access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities."

3.2. Nuclear security: An international priority

There is an international consensus that responsibility for nuclear security within a State rests entirely with that State as it's a matter of national security. Furthermore each State has its specific context and evaluation of the threat. However, the threat of nuclear terrorism has been recognised by all States as a matter of great importance, which explains the growing need for international cooperation and exchange of good practices to carry on the enhancement of nuclear security.

3.3. History and instruments on nuclear security

From the beginning of the 1970s, the IAEA has served as a forum where experts have been able to exchange their national experiences in the field of physical protection of nuclear materials. The outcome of the different discussions and exchanges was issued in a document entitled "The Physical Protection of Nuclear Material" in 1972 (with subsequent revisions of this document being published as IAEA Information Circular: INFCIRC 225). The document was written in the form of recommendations with a technical and evolutionary character.

These recommendations were followed by the development of a Convention on the Physical Protection of Nuclear Material (CPPNM), under the auspices of the IAEA, opened in 1980 for the signature of States, and entered into force on February 8th 1987. By ratifying the CPPNM, contracting parties take commitment to develop and implement a nuclear security legal framework.
An Amendment to the CPPNM, signed July 8th, 2005, significantly widens the reach of the CPPNM, while the initial text essentially concerned the protection of nuclear materials during international transport to the domestic use of the nuclear materials (in installations, in storing and in the course of transport). The Amendment also concerns the protection of nuclear materials and nuclear facilities against sabotage. All EU Member States as well as the European Atomic Energy Community (EURATOM) are contracting parties of the 1980 Convention and have participated to the negotiation of the Amendment to the CPPNM. This Amendment has not yet entered into force.
In particular, the Amendment brings up the first responsibility of States in protecting nuclear materials and nuclear facilities against theft or sabotage. It requires however that the physical protection system implemented in every State applies the Fundamental Principles of Physical Protection of Nuclear Material and Nuclear Facilities, insofar as is reasonable and practicable.
This Amendment provides a more effective tool appropriate to meet the expectations of society in considering the risks of malevolence or of terrorism. By ratifying this Amendment, States undertake a commitment to ensure the security of nuclear material in domestic storage, use and transport and of its nuclear facilities (including NPPs).

It has to be emphasised that EU Member States contribute permanently to the IAEA efforts and promote the CPPNM in all their international relations.

With the same overall objectives, the Security Council of the United Nations Organisation decided to adopt specific resolutions against nuclear terrorism:

- The Resolution 1373, adopted in 2001 after the 9/11 attacks, requires member states to take measures tending to fight against the terrorism and to control their borders.

- The Resolution 1540, dealing with Weapon of Mass Destruction was unanimously adopted on April 28th, 2004. It is legally binding, and implies in particular a change of the legislation of member states. It decides that States shall refrain from supporting by any means non-State actors that attempt to acquire, use or transfer nuclear, chemical or biological weapons and their delivery systems. It reaffirms the interest of an international cooperation in civil nuclear energy. In particular, it requires States to maintain "appropriate effective physical protection".

In September 2005, the International Convention for the Suppression of Acts of Nuclear Terrorism was opened for signature and on July 7th, 2007 it came into effect. It is primarily an international criminal law instrument that defines certain acts as criminal offences and obliges States Parties to establish their jurisdiction over such offences, to render them punishable under their domestic law and to provide for extradition or prosecution of alleged offenders. However, it also obligates States Parties to protect radioactive material (including nuclear material), taking into account IAEA recommendations (which include INFCIRC 225).
Even if nuclear security is the responsibility of States, the universal adherence to and full implementation of international nuclear security instruments is needed.

3.4. The central role of IAEA

As part of its efforts in nuclear security, the IAEA's Board of Governors has approved a series of Nuclear Security Plans that set out the IAEA programmes for nuclear security. One component of the Nuclear Security Plans has been the development of the Nuclear Security Series of documents which provides nuclear security fundamentals, recommendations and implementing and technical guides for Member States to assist them in implementing new nuclear security regimes, or in strengthening existing regimes.

The Nuclear Security Series is designed in a tiered approach with:

- the Fundamentals-level publication providing the overall Objective and Essential Elements for the entire regime,
- the Recommendations-level publications outlining what a regime should do in specific areas of nuclear security,
- and the implementing and technical guides publications providing detailed guidance about how to establish specific nuclear security systems regimes and measures.

3.5. IAEA Nuclear Security Recommendations

At the recommendations level, one key document is the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) which has the objective to achieve effective physical protection against the theft or unauthorised removal of nuclear material and against the sabotage of nuclear facilities and transports.

The recommendations in INFCIRC/225/Revision 5 relate to:

- the objectives of a States' physical protection regime; the elements of a States physical protection regime for nuclear material and nuclear facilities;
- the requirements for measures against unauthorised removal of nuclear material in use and in storage;
- the requirements for measures against sabotage of nuclear facilities and nuclear material in use and in storage;
- and the requirements for measures against unauthorised removal and sabotage of nuclear material during transport.

Such requirements involve the prevention (first line of defence), the detection (second line of defence), the response (third line of defence) and mitigation or recovery procedures (fourth line of defence).

Implementing guides or technical guidance documents give detailed advice on how to implement the recommendations. For instance these documents deal with topics such as threat assessment, vital area identification, security of transport, internal threat (insider) and nuclear security culture.

3.6. IAEA Training and Advisory Services

An objective of IAEA is also to strengthen the capability of States to assess the vulnerability of their nuclear facilities to possible malicious acts. This will be achieved by providing, on request, assessment services, together with associated advice and follow-up actions to improve security arrangements at specific locations, by the development of the appropriate methodologies, by the provision of training and through other supporting activities.

In this field, the IAEA offers a system of peer review of State regimes and nuclear facilities physical protection through the International Physical Protection Advisory Service (IPPAS). IPPAS not only provides States with advices to help strengthening the effectiveness of their physical protection systems but also identifies good practices. This service covers the interface between safety and security (see section 5.2).

IAEA provides additional peer review services such as the Integrated Regulatory Review Services (IRRS). When a security module is included in the IRRS scope, at the choice of the hosting country, it might also provide valuable insights about the robustness and adequacy of the nuclear security regulatory regime of that country.

3.7. Nuclear Security Summit 2012

The importance and necessity of nuclear security worldwide was stressed again at the Nuclear Security Summit (NSS) in Seoul in March 2012. The scope of the NSS is much broader than only the security of NPPs. However, a number of the statements addressed in the NSS Communiqué include recommendations identical or very similar to those discussed by AHGNS:

- The importance of countries' ratification of CPPNM and its amendment, and of implementation of IAEA's INFCIRC/225/Rev.5 in their national practice

- Recognition of the essential role of IAEA and its Nuclear Security Plans

- Encouragement to make use of IAEA's activities to assist national efforts to enhance the nuclear security infrastructure

- That nuclear safety and security measures should be designed, implemented and managed in a coherent and synergistic manner at nuclear facilities

- That emergency plans, response and mitigation capabilities should address both nuclear safety and security

- The importance of developing and enhancing a nuclear security culture including all stakeholders by education and training

- Enhancement of information security and cyber security to protect nuclear facilities from malicious act

- The importance of sharing best practices on bilateral as well as multilateral basis

3.8. The European Nuclear Security Regulators Association (ENSRA)

Since the second half of the 1990s, an informal group of European governmental regulatory authorities involved in nuclear security have met to share their views and experiences in their field of competence. To strengthen the network and in view of the importance attached to the security of nuclear material and nuclear facilities, the ENSRA was founded in 2004 (Madrid), modelled on a similar group of European safety authorities, the Western European Nuclear Regulators Association (WENRA). Currently, the regulatory bodies of the following states are members of the ENSRA: Belgium, Czech Republic, Finland, France, Germany, Hungary, the Netherlands, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

The objectives of the ENSRA are:

- to facilitate confidential exchange on nuclear security matters
- to provide the IAEA and other official bodies with a source of expert advice
- to develop a comprehensive understanding of the fundamental principles of physical protection
- to promote and achieve a common approach in nuclear security within Europe
- to establish professional competence in the field of nuclear security.

4. GOOD PRACTICES FOR NPPS IDENTIFIED BY AHGNS

4.1. Summary of results of the questionnaire

As mentioned in section 2.1 the Polish Presidency prepared a questionnaire in order to obtain the necessary information from Member States in the field of the nuclear security. The analysis of their replies has shown that all Member States have established a nuclear security regime based on the principles of the CPPNM with its Amendment and IAEA recommendations. The nuclear security regimes are commensurate to the extent of the nuclear industry in each State.

The 32 good practices in accordance with the scope of the mandate do not take into account parts of the replies that depend on national circumstances, legal or administrative systems. Moreover, they do not in any way reflect an assessment of existing national security regimes in the EU and they could apply without prejudice to Member States' specific characteristics (e.g. the extent of their nuclear sector or their administrative organisation) and circumstances.

The implementation of good practices has to take account of national administrative and institutional arrangements as well as to the extent and nature of national nuclear sectors.
In several instances the need to ensure consistency between safety and security measures as well as to effectively take into account the multiplicity of actors, public and private, involved at all levels is stressed. While in several instances the good practices are in substance equivalent to those presented in IAEA reference documents or in provisions of the CPPNM with its Amendment these good practices remain valuable as they derive from the experience drawn in implementing international guidance.

4.2. Identification of good practices

The 32 good practices set out at Annex I can be grouped into two broad categories: those which relate to the national legal and regulatory framework (bullet i to iv below) and those which relate to the implementation and maintenance of a nuclear security regime (bullet v to x below). Without prejudice to the full text of the good practices and to the relevance of each and every of them the section below intends to sum up their main elements.

i. While defining the legal and regulatory framework for nuclear security, as required by the CPPNM with its Amendment it is ensured that interfaces with other legal and regulatory frameworks (such as radiation protection, safety, transport of dangerous goods, safeguards, non-proliferation, etc.) are duly considered and managed.

ii. The State carries out the definition and assessment of the threats to the NPPs, be it through the design basis threats (DBT) or the threat assessment[1] . Several experts from different organisations with expertise in the field of intelligence, law enforcement and nuclear security work closely together and are involved in the threat assessment process. Moreover the threat assessment is formally reviewed on a regular basis or whenever deemed necessary, and if necessary the DBT is updated.

iii. The nuclear security regime is regularly assessed in order to verify its efficiency and its consistency with the development of international instruments, lessons learned from significant events and changes in the DBT or threat assessment.

iv. Mechanisms for the exchange of information among various actors of nuclear security are implemented to guarantee the confidentiality, integrity and availability of information. To ensure that sensitive information is appropriately protected such mechanisms are based on a national system of information classification.

v. It is essential to take into consideration the nuclear security requirements at a very early stage in the life-cycle of any NPP starting at the design stage. Similarly, nuclear security measures have to be implemented from the construction stage and their tests be completed prior to the placement of nuclear material on-site. It may be necessary to consider that the threats may evolve during the development of the project from design to operating stage.

vi. The performance of its nuclear security systems is demonstrated by the operator and evaluated by the State. In this respect, it is considered that technical expertise to perform this evaluation at a State level is necessary, including capacities to test components of nuclear security systems implemented at NPPs.

[1] For this purpose, the IAEA implementing guide "IAEA Nuclear Security Series N0 10 Development, Use and Maintenance of the Design Basis Threat" may be considered

vii. The operator of NPPs implement measures, supported by a strong management system, to ensure that security systems remain effective and in accordance with conditions set by the competent authority, report failures and take corrective measures. In this respect regular maintenance, verification tests and exercises as well as review of existing physical protection systems according to evolutions of the DBT or threat assessment are key components and are performed according to approved procedures and schedules. Regular inspections are carried out by the competent authority.

viii. Notwithstanding the operator's prime responsibility for the implementation of nuclear security on its NPP (e.g. physical protection structures and devices, on-site procedures, contingency plans), the operator and the State coordinate as regard to prevention/detection and intelligence measures as well as in term of response mainly in situations involving threat within and beyond the DBT, when additional response resources may be necessary in order to complete forces and resources at operator level.

ix. Screening of persons to assess their trustworthiness in order to determine, in a graded manner, the areas in the NPP and category of nuclear material and of information to which they may have access, appears to be an effective mean to reduce insider threat. Special attention is paid to temporary personnel. In this respect the operator may rely on State organisations to obtain information for the screening.

x. Nuclear security culture is an essential component of the security of NPPs. The nuclear security culture is promoted at all levels by operators and State. Several national legal and regulatory frameworks have requirement related to the security culture. All people, including top level managers, involved in the design and operation of an NPP must be fully aware of their responsibility for the security of the plant.

5. SELECTED THEMES FURTHER ELABORATED ON BY AHGNS

During the Danish Presidency the AHGNS selected five themes for further discussion and elaboration within the group. The five themes were selected based on topics highlighted in the conclusions of its interim report, the mandate of the AHGNS and with the aim of AHGNS being able to add value to the already existing good practices/guidance on these subjects.

5.1. Computer Security/Cyber Security

5.1.1. Context

Regarding threats connected with cyber security and the key role of Information and Communication Technology (ICT) systems and Instrumentation and Control (IC) systems[1] in any NPP, high priority has to be assigned to cyber security. As in other areas of nuclear security it is the Member States' responsibility to ensure reasonable protection against malicious acts caused by cyber attacks, if these attacks can have unacceptable radiological consequences. An analysis of all relevant threats must be done by the Member States, preferably in line with the principles for the DBT process as it is used for nuclear security in general. The threat analysis should include but not be limited to the possibility of combined attacks using both cyber and physical means (e.g. cyber attack on physical protection systems to support subsequent "physical attack").

In order to protect NPPs appropriately against the identified cyber threats, protection measures need to be applied. The decision on the level of protection sufficient for reasonable protection lies with the Member States. The decision should be based on an evaluation of risks which includes insider threats and the fast evolving nature of cyber threat.

When dealing with cyber threats against NPPs it is important to look at the overall use of IC/ICT systems at the plant e.g. their interfaces and interdependencies and the information contained in different systems. All IC/ICT-systems and components of an NPP may be grouped and protected according to the potential direct or indirect consequences on the safety or security of the plant in case of a cyber attack on these systems.

[1] Information and Communication Technology (ICT) systems and in Instrumentation and Control (IC) systems, here after referred to as IC/ICT systems.

5.1.2. Risk model

A very basic risk model can be used to periodically evaluate risks, once appropriate protection measures have been suggested. Risk, in this IC/ICT context, is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization[1], the people or the environments.

The model is based on the following components:

- Target identification – no matter whether it is IC/ICT-systems, information, or it is the plant itself, it is necessary to identify critical assets that can be targets.

- Relevant threats definitions: threats to assets are identified in line with the threat assessment process and DBT (attributes and characteristics of adversaries).

- Risk assessment: considering the identified threats, risks are assessed and the appropriate technical and organizational measures are implemented in order to prevent an attack and to mitigate its consequences.

- Control and sustainability: the mechanisms necessary to test performance, maintain the effectiveness and to review the protection measures in place on a regular basis.

Risk assessment is a method to analyze the residual risk when applying protection measures.

When it comes to IC/ICT-components in Critical Infrastructure, critical components include Industrial Control Systems (ICS) and especially Supervisory Controls and Data Acquisition systems also called SCADA – systems which also include systems for operating, controlling, managing and monitoring an NPP. There can be several SCADA systems in an NPP which are not necessarily interconnected.

[1] ISO/IEC 27005.

Many industrial control systems consist of legacy technologies that are integrated with new systems and technologies. IC/ICT-security mechanisms may not have been integrated with the systems from the beginning, and the risk level can rise when different systems are integrated in a way that they were not originally designed for. So, it is necessary to follow a strong policy that enforces a timely review of all NPPs concerning the status of their IC/ICT-security. Subsequently, where not yet introduced, appropriate security measures including change-management and measures to keep the overview of the systems interconnectivity should be implemented.

An appropriate level of protection must be used for all IC/ICT-systems of an NPP including computer systems within NPPs that contribute to the physical protection (access control systems, surveillance systems etc.) or holds sensitive information (including nuclear material accountancy data) of the site. Although cyber threats are usually seen as external the potential role of insider threats should be taken into account given that insiders can have access to on-site systems.

5.1.3. Cyber threats affecting NPPs

The threats affecting IC/ICT systems are threats, with varying level of consequences, against:

- Confidentiality – unauthorized access to or interception of information.
- Integrity – unauthorized modification of information, software, hardware etc.
- Availability – blockage of data transmission lines and/or making systems unavailable.

The three issues have to be held up against each other and their importance evaluated.
The threats pointed directly at IC/ICT-systems can be internal as well as external: forged firmware, infected service devices, USB storage devices, worms, virus, theft of knowledge and confidential information, distributed denial of service attack, social engineering, etc. States should consider including such threats in the national DBT as a way to address the threats. Besides, given the importance of the human factor in security breaches, due consideration of cyber-related issues should be an integrated part of nuclear security culture.

The implementation of well defined security mechanisms and policies in addition to network overview would help keeping a stable and low risk level.

5.1.4. A risk management approach for NPPs

It is recommended that NPP operators implement a risk management approach for all computer systems which take into account the guidance in IAEA Nuclear Security Series No.17 and which, once these systems have been comprehensively inventoried:

- Identifies and characterises threats to these systems
- Identifies the potential impact on the NPP of the threats to each system, taking advice from safety specialists where necessary
- Applies an appropriate level of security measures to each system, based on a graded approach related to its potential impact and the value of the asset
- Ensures the residual risk to these systems has been reduced to an acceptable level
- Documents the implementation and outcome of the risk management process

National regulatory authorities should inform operators of the national threat assessment to IC/ICT-systems and should review the risk management documentation produced by the operator.

Periodic reviews/audits of the IC/ICT-systems of the NPP could be regularly undertaken based on national guidance. It could also be useful for EU Member States to have their information systems audited as part of their IPPAS missions.

5.1.5. References on cyber/computer security

From an IC/ICT-system security perspective a number of standards and guidelines have been set. Issues regarding cyber security and security of the Critical Information Infrastructure can be used for establishing a basis for a structured and measurable IC/ICT-environment for nuclear facilities:

- EU (Council Security Committee) policies and guidelines for protecting classified information
- COM (2009) 149 on Critical Information Infrastructure Protection followed by
- "Achievements and next steps: towards global cyber-security" - COM(2011) 163
- ENISA work on protecting industrial control systems

- International standards for information security management (i.e. ISO/IEC 207000 series)
- ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security (part 1-3).
- Process control and SCADA security - good practice guidelines from the British CPNI

Especially prepared for nuclear facilities are:

- IAEA Nuclear Security Series, No. 17, Computer Security at Nuclear facilities
- IAEA Nuclear Security Series No. 10, Development, Use and Maintenance of a DBT
- Regulatory guide 5.71 Cyber Security Programs for Nuclear Facilities (US Nuclear Regulatory Commission)
- North American Electric Reliability Corporation (NERC) Standards on Critical Infrastructure Protection (CIP)
- WINS Best Practice Guide, Security of IT and IC Systems at Nuclear Facilities

5.1.6. Conclusions

AHGNS emphasizes a set of findings to be considered by regulators for all IC/ICT-systems which may affect safety or security of the NPP:

- NPP management is responsible for creating and maintaining an information security policy and security management system.
- The design of these systems must ensure that if a single system fails, the overall security and safety of the facility must not be affected. The design must include protection systems, which must be independent of other systems.
- The computer systems which are related to safety or security of the plant must be physically separated from any other computer network.
- Strong policies for change-management and implementation of security mechanisms are required, in particular in order to keep the overview of the systems interconnectivity.
- In light of the increased relevance of cyber threats, review/audit of NPP concerning the status of their IC/ICT-security is advisable, using notably IAEA guidance as benchmark. In this regard, it could be beneficial that the IPPAS mission could cover this issue.

- All kind of operations requiring access (internal as well as external) to computer systems for operational issues including maintenance must be highly controlled and conducted by personnel who have received a thorough security screening.
- Plan regularly intrusion and vulnerability tests and audits, either in the actual installations or in simulated environments.
- Ensure an adequate education of personnel with planned updating courses.
- Computer system hardening should be considered to all systems.
- Information security should be considered at all stages of the lifecycle of the NPP.

5.2. IAEA's International Physical Protection Advisory Service (IPPAS) Missions

5.2.1. Context

AHGNS has already in its first term in the fall 2011 identified good practices for nuclear security, among those the value of IPPAS missions. In 2012, this subject has been further elaborated on with a presentation from the IAEA, a presentation from a mission team leaders experience and presentations from Member States which have experiences with IPPAS missions. All Member States agree on the great value of these missions both with respect to the quality of the mission report and the process itself which gives the opportunity for a Member State to look back at its own regulations and procedures.

AHGNS acknowledges that IPPAS missions are important in providing in-depth evaluation of Member States` physical protection regime and in promoting nuclear security culture and developing its sustainability. It should be noted that IPPAS missions are without prejudice to Member States` entire responsibility for the establishment, implementation and maintenance of a physical protection regime.

5.2.2. The IPPAS process

The IPPAS mission is fundamental to IAEA programs for improving States' nuclear security regime. The objectives of IPPAS missions are to

- Review States` physical protection regime and compare it with international legal instruments, recommendations and guidance.

- Assist States and nuclear operators to implement requirements of international instruments and recommendations of INFCIRC/225/Rev.5.

- Identify good practices that could be communicated to other States for long-term improvement.

The IPPAS scope can be divided into two levels:

- **The State level** which deals with the institutional organization, assignment of responsibilities, international obligations and cooperation, the integration and participation of other organizations (law enforcement agencies, etc.), checking primary and secondary legislation, roles and responsibilities of the competent authority, the licensing/authorization process, and the threat assessment and DBT.

- **The facility level** which deals with security management and planning, security procedures and culture, security assessment capabilities, protection systems (by design, in operation) be it technical systems for physical protection or control systems.

A mission is requested by a State and consists typically of an informal preliminary meeting, a formal request, a preparatory meeting, the mission itself, a final mission report and eventually a follow-up mission. It is performed by an international multidisciplinary team of experts brought together by IAEA. The mission itself lasts from six days to two weeks and involves a team of four to six experts and an IAEA technical officer, under a team leader.
The outcome of the mission, the mission report, contains recommendations, suggestions and good practices and is held confidential. The follow-up is based on the recommendations in the mission report and includes additional advice such as legislative advice, proposal on training for regulators and operators, suggestions on threat assessment methodology.
Whilst the way recommendations are presented is important if they are to be accepted and implemented by the Government, the report can be openly critical without the need to consider how this will be interpreted by the public. The mission reflects the quality of the IPPAS team and should be conducted in a climate of mutual trust while respecting confidentiality requirements.

5.2.3. EU Member States' motivation for an IPPAS mission

There are several motivations for an EU Member State to have an IPPAS mission, these include:

- The value of a mission, and the whole process around the mission, as a useful peer review instrument.
- The benefit from a peer checking by foreign experts with a broad knowledge in nuclear security.
- The national good practices identified will be internationally recognized by the mission team.
- The opportunity for the EU Member States regulatory authorities together with the mission team to look back at their approach to security.
- Allows comparison between EU Member State legislation/regulations and the practice on the ground, raising questions as to the adequacy of law, regulatory guidance and enforcement.
- Valuable independent expert views and recommendations, which could be used to justify proposals to the government for the further strengthening of the physical protection regime.

Reports and their recommendations are generally well received and implemented. Missions do contribute to confidence building, and it stimulates cooperation among authorities and stakeholders within the EU Member State. A mission also acts as an "eye opener" in allowing those engaged to look at things not done on a daily basis which may lead to adjustments and possibly lead to self-assessments and the identification of areas, where IAEA guidance/recommendations should be amended.

5.2.4. Conclusions

The nuclear security regime in EU Member States should be reviewed on a regular basis. AHGNS recognizes the IPPAS missions as the international instrument for improving security not only at NPPs, and notes the following:

- IPPAS missions should become the norm for nuclear security evaluation for EU Member States with established and planned NPPs.
- EU Member States with NPPs which have not yet invited IPPAS mission should be encouraged to do so.

- IPPAS missions should be carried out in all EU Member States with NPPs on a regular basis (for example every 10 years while taking due account of the need to adapt this time period to ongoing activities of the stakeholders involved).
- All missions should have a follow-up mission. The time span between the mission and its follow-up could vary from Member State to Member State and should depend on the recommendations and suggestions given in the IPPAS mission report. However, follow-up missions three years after the initial mission should be normal practice.
- The security relating to cyber threats should be part of the scope of a mission as has already been the case in some recent missions.
- Best practices identified through the different IPPAS missions should be widely shared at the European and international level and the implementation of such practices should be promoted by the IAEA.
- It is up to an EU Member State to decide on the opportunity to inform the public about the organization and main findings of the IPPAS mission it has requested.

5.3. Intentional Aircraft Crash

5.3.1. Context

The **accidental** crash of an aircraft has been considered during the design-phase of several of the Member States' NPPs. Accidental crashes are considered to be possible. Several safety measures have been introduced to cope with the consequences of such accidents. Also NPPs which have not been especially designed against aircraft crashes provide a certain resistance by design, like separation of redundancies, emergency cooling-systems, etc.

After the terrorist attacks of September 11th, 2001, an **intentional** aircraft crash – especially using commercial aircrafts – became of worldwide interest. Moreover, taking into account circumstances and consequences of those attacks, in the context of nuclear security, specific measures for the prevention of intentional aircraft crashes are of high significance.

The following text will only focus on intentional attacks being neither part of the State's DBT nor basis for the constructional design of the NPP. At the same time, it is understood that any additional security measures should be designed, implemented and managed in a coherent and synergistic manner with safety measures.

5.3.2. Countermeasures against intentional aircraft crash as beyond DBT event

Even if the aircraft attack against an NPP is not part of the DBT, there is a common understanding among Member States that dedicated countermeasures need to be implemented.

First, this specific kind of threat benefits from general measures implemented in order to help prevent RENEGADE-situations[1], while specific dedicated countermeasures could also contribute to mitigate the consequences of an intentional aircraft crash, in particular by timely activation of emergency procedures.

Gathering of relevant intelligence information is of primary importance so as to assess and anticipate threats and adapt protection measures to be implemented. It constitutes a first line of defence in terms of a defence-in-depth concept.

The international aviation security regulations (cf. e.g. Regulation (EC) 300/2008) also constitute an effective tool as a second line of defence. These measures mainly aim at the prevention of hijacking scenarios. Moreover, standard flight safety measures are another tool to keep RENEGADE-scenarios to a minimum.

However, Member States also agree that further security measures should be implemented within the framework of the State's nuclear security regime.

The timely warning of NPP staff of a potential imminent aircraft attack was identified as one of these measures. Such warning can be assured by coordination with those authorities responsible for civilian or military control of airspace either nationally or internationally. Provisions should be taken so that NPPs potentially threatened are alerted as soon as possible in case of a confirmed RENEGADE-aircraft.

NPP operators should introduce a set of measures to mitigate the consequences of an intentional aircraft-crash, including fire protection capabilities (man-power, equipment, etc.).

Emergency plans, which can be easily activated in case of a RENEGADE-alert must be prepared and regularly tested by the relevant authorities.

It is regarded valuable to have a graded approach in preventive measures depending on the confidence of the RENEGADE warning/alert (warning levels).

These different warning levels can also be used to increase the on-site preparedness when intelligence gets knowledge on specific planning or preparation of an attack on an NPP.

Trainings of procedures (emergency planning and means of communications) as well as tests of warning/alerting channels and alert plans are particularly important and should be performed on a regular basis.

---

1 RENEGADE means the hijacking of civil aircrafts to be used for intentional aircraft crashes

5.3.3. Conclusions

The AGHNS regards the following set of good practices as helpful for Member States operating NPPs:

- Competent authorities should have a firm understanding of the potential consequences of an intentional aircraft crash as a basis for countermeasures.
- Measures and procedures for timely warning and alerting the NPPs in case of identification of a RENEGADE-aircraft potentially threatening them should be considered at national level.
- Operators should supplement existing emergency plans so they include accidental or intentional aircraft crashes. Differentiated alerts ("specific warning levels leading to specific measures") should be considered.
- Competent authorities should provide information based upon threat assessment to the operators of NPPs as fast as necessary.
- Operators together with the relevant authorities should perform regular training exercises of procedures, means of communication and alert plans.

5.4. Nuclear Emergency Planning: Synergies and consistency between Safety and Security

5.4.1. Context

One possible result of a nuclear security event could be a safety issue at an NPP. On the other hand, emergency situations caused by safety events may lead to a security issue.

As safety and security events can lead to one another, emergency plans and contingency plans for NPPs must be consistent and synergies should be drawn between the areas. Such consistency can minimise the consequences of a nuclear incident or accident for the population and the environment, regardless of initiating event, by minimising potential conflicts between planned actions, information sharing, improving effective allocation of resources and exploitation of synergies. These principles are reflected in the CPPNM Amendment[1] and INFCIRC 225 rev. 5[2].

[1] Fundamental Principle K - ***Contingency Plans*** – "*Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all license holders and authorities concerned."*

[2] See paras 3.58-61 and 5.44-58 of INFCIRC/225 Rev.5

5.4.2. Practice

To avoid confusion amongst responders, mistakes in handling the response or potential delays, inconsistencies in the emergency plans and contingency plans should be removed. These plans should be consistent particularly in terms of:

- Understanding of the different operational responses needed for each type of event.
- Coordination between the safety and security elements of the response.
- Cooperation between response organisations.
- Understanding and harmonizing of technical terms for both emergency and contingency plans.

By proper considerations in the emergency plans an appropriate level of site security must be ensured even during emergency situations.

Contingency plans should be prepared at three levels: on-site; off-site at the local level; and at the national level both by operator and State to effectively respond to the assumed threat. Contingency plans must be tested via exercises comprising scenarios including safety and security issues.

The on-site contingency plan should be prepared and implemented by site operators and should include the guard force under its responsibility. It should ideally focus on the prevention of any actions leading to radiological consequences. On-site plans should be approved by the Member States competent authority.

At the local level, off-site, the contingency plan should be prepared and implemented by local State representatives in liaison with local responders. Contingency and emergency plans must cover, as appropriate, communication with the public (e.g. warning and informing), counter-measures off-site (e.g. evacuation and sheltering), treatment of casualties, and the policing response and investigation.

The National level contingency plan should be prepared and implemented by competent authorities, including Ministries, in charge of:

- nuclear security;
- nuclear safety and radiation protection;
- response forces and especially counter terrorism units;
- criminal inquiries and forensics;
- legal affairs.

Contingency and emergency planning at the national level should cover deployment of national capabilities, (including military support if appropriate), national level radiation monitoring, international notifications and, as appropriate, engagement with parliaments as well as nationwide public/media engagement.

All these plans should be closely connected with each other.
Authorities in charge should work in close cooperation with Ministries, operators and Competent Authorities in charge of nuclear safety and emergency response. Special provisions have to be taken, both in contingency plans and in emergency plans, to coordinate the multiple actors involved in situations resulting from malevolent action.

Whenever necessary, decisions related to responses have to be taken at the lowest appropriate level with the local and/or regional authority seeking advice and direction from the State authorities on issues of national significance.

5.4.3. Conclusions

In light of the above the AHGNS has identified a set of findings to be considered by regulators:

- It has to be ensured that even in case of an emergency situation the site security is on an appropriate level.

- Reflecting international commitments and recommendations, contingency plans to counter threat and plan responders' actions should be established and implemented at operator and State level. Contingency plans and emergency plans prepared to avoid or minimize the consequences of a nuclear incident or accident for the population and the environment must be comprehensive and consistent.
- Authorities in charge of contingency planning must liaise with authorities in charge of nuclear safety and emergency response to ensure the consistency.
- Contingency plans must be tested via exercises comprising scenarios mixing safety and security issues.

5.5. Exercises and Training

5.5.1. Context

There is a clear need to set up certain requirements for the security organisations of NPP operators so as to ensure the effectiveness of arrangements for nuclear security. These include the definition of responsibilities for the implementation of the nuclear security arrangements in particular with respect to exercises and training policies.

The operators of NPP should define a policy of security exercises and security vocational training that should meet the requirements set by the competent security authority even though there may be differences between Member States regarding the conduct of these exercises. Its implementation should be mandatory for the operator. Other appropriate arrangements should also be in place for other authorities concerned with nuclear security. Within this policy, exercises help to identify margin for improvement and contribute to the strengthening of nuclear security.

Exercises need to be carried out at both a table-top and on-site level, using combined safety and security based scenarios. Therefore, there is a clear need to ensure that live on-site training is also carried out. During on-site training it is important to find out the real response times of different responders. The scenarios should be created taking into account the DBT. During the exercises special attention should also be given to communication between actors and the chain of command, as several responders are involved, and public relations.

To verify the effectiveness of the security arrangements and the operators' security organisation, it is important to carry out unannounced exercises, however taking appropriate precautions to prevent misunderstandings related to the status of the exercise. This can be carried out in co-operation between the operator and national authorities.

5.5.2. Exercises Conducted at Nuclear Power Plants

The policy of nuclear security drills should be defined by the competent authority for nuclear security and implemented by the operator in charge of a NPP for its part. This policy should be set out in arrangements, including those regarding the national policy of defence and security exercises. It is of vital importance that the regulation establishes some obligation for the operators with regard to exercises and determines the set of potential threats to be taken into consideration. The authorization files should contain the program of vocational training. In addition to the obligations set by the state, the operator for his part should draw up a policy of exercises which he reports to the competent authority.

The exercises on the NPPs deal primarily with the protection and security of the NPP itself and not with the stocktaking of nuclear material in crises situation.

The practice, vocational training and the real-life situation relevant for the security stakeholders should be regularly monitored both by the security authority and by the operator. Their conditions of implementation should be described in the file needed to obtain the authorization to operate a NPP.

Furthermore, common training and exercises between the security organizations of the operator and relevant national authorities is a key issue. This is because different authorities may have special tactics and use special terminology; therefore, it is important to arrange exercises involving all responders.

Three categories of exercises and their objective related to protection can be considered:

Type 1 exercises performed at operator level with the internal security forces. These exercises are aimed at assessing the response procedures, based on internal and external threats, including the presence of explosives.

Type 2 exercises involving the territorial police. These exercises focus on response procedures of the territorially competent police forces, the reaction to acts of trespassing, the management of interfaces between actors inside and outside the site.

Type 3 exercises are developed at national level and involve all the security stakeholders. These exercises involve the special forces dedicated to NPPs. Their aim is to evaluate the organization and implementation of security plans as a whole, the interfaces between the authorities and the operators, the command posts location and equipment, the communication framework with the public and the media. They are interested in the coordination of responsiveness capabilities, the warning periods and conditions for mobilizing the resources deployed. They ensure the faultless balance between protection and intervention plans and contingency and emergency plans.

Arrangements must set the frequency of exercises according to their category. It is advisable that exercise of type 1 is conducted quarterly as well as an annual exercise of type 2. Type 3 exercises should be conducted preferably every 18 to 24 months on a NPP or other facility designated by the nuclear security authority in conjunction with the operator. They can be less frequent because their design is the result of a complex working activity which takes several months while their implementation involves all actors of nuclear security (operator, protection forces internal to the site, territorially competent police forces, local authorities and judicial authority). It also ensures the participation of the safety authority's representatives.
The policy of exercise is therefore in keeping with a perfectly defined framework and meets specific objectives. It is the subject of control by different authorities or hierarchical levels, contributes to an ever increasing security level and helps designing lines of effort in conjunction with the identified ways of improvement.

5.5.3. Training

Only a person trained as a guard, as specified in the relevant national regulation, or with some other security-field training, can act as the shift manager or a security guard. In addition, security personnel should be required to fulfil the general conditions stipulated for an approved guard force. Basic training to carry out security guarding duties can be given during the security guard training in accordance with the national regulation. Specific nuclear-facility training should be required before the person can act as a member of a facility security organisation. A guard shall have a valid and approved training in the use of force, including weapons where guards are authorised to carry them. Documentation of the training provided should be required.

In regular training events and demonstration tests (practice and theory), shift managers and other security personnel shall demonstrate their capability to carry out their guarding duties correctly and safely. Demonstration test and training events should be described in an annual training programme. The competent authority should monitor the training programme and its execution. Records of the demonstration tests, training and participants should be kept.

Training of security personnel should be arranged by the operator in cooperation with the private guarding services supplier (if such a supplier is used) according to the training programme.

5.5.4. Conclusions

In the end it is important to create a system that takes into account the special conditions of the Member State where the NPPs exist. For example, special police units are responsible for nuclear security in some States, whereas in other States there are arrangements where several authorities are jointly involved. It is important to recognise what kind of system is best fitting the national system, legislation and resources.

In summary, certain issues should always be considered:

- Legislation and requirements set by the competent authority regarding security organisation and security personnel (including training, mental and physical capabilities)
- The responsibilities and the roles and competences of all stakeholders should be clearly defined
- Basic and advanced training (both table-top and on-site) of security personnel including joint training with national authorities
- Special conditions of the State where the NPP is located, including resources of different authorities, response times of authorities as well as special capabilities of different authorities
- Joint safety and security based scenarios, including preparedness arrangements
- Monitoring, evaluating, reporting and developing training and exercises by learning from the previous ones
- Following global incidents and trends in the nuclear security area and learning from them

6. DIALOGUE WITH NEIGHBOURING COUNTRIES

Based on the mandate of AHGNS a full-day meeting was held with those of EU's neighbouring countries which either have or are planning to construct NPPs. The meeting took place on 11 April 2012 in Brussels.

Security experts from Russia, Belarus, Switzerland, Turkey and Ukraine accepted the invitation send from the Presidency and participated in the meeting together with representatives from IAEA.

At the meeting a general overview of the work of the AHGNS was given.

The importance of the ratification of the CPPNM (and not least the Amendment from 2005) was especially underlined.

The correspondence between the goals of the work in AHGNS and the Seoul Nuclear Security Summit Communiqué from March 2012 was outlined. IAEA expressed that they were pleased with the high level of political support from the Nuclear Security Summit to IAEA's leadership within nuclear security.

At the meeting, IAEA representatives presented some of the IAEA security tools and stressed the necessity of integrating security and safety measures in future work regarding NPPs. The differences between IRRS and IPPAS missions were outlined – the IRRS-missions are concerned with the regulatory measures within a state, while the IPPAS-missions are "the complete package".

Furthermore, the importance of implementing a strong nuclear security culture was emphasized by IAEA.

Russia and Switzerland gave presentations on their nuclear security regimes. All countries expressed their support of and cooperation with IAEA. Russia has, as the only neighbouring country, the full cycle of nuclear processing from production of nuclear fuel to permanent storage of nuclear waste, and Russia works as consultant to a number of neighbouring countries.

It was stressed that the final AHGNS report, unlike the interim report, will be public, and therefore could be shared with the neighbouring countries following its release in June 2012.

Finally, the possibilities for continued contact and cooperation between the EU and its neighbouring countries on the subject of nuclear security were discussed. In general the neighbouring countries expressed a positive interest in a further exchange of views and cooperation with the EU Member States. Additionally, all countries present at the meeting agreed on the necessity of international cooperation based on the IAEA's recommendations and guidance on nuclear security matters.

7. MAIN CONCLUSIONS AND RECOMMENDATIONS

7.1. Main Conclusions

The 32 good practices (see section 4 and Annex I) identified in the 2nd semester of 2011 should apply to any Member State taking due account of its specific characteristics and circumstances.

Five selected themes were chosen for further elaboration in the 1st semester of 2012 (see Section 5). The work conducted allowed to precise and complete the AHGNS findings regarding the nuclear security of NPPs.

Finally, the AHGNS has drawn nine main conclusions. These main conclusions are aimed at all entities involved in nuclear security and will according to AHGNS, if given adequate consideration, contribute to ensure a higher level of nuclear security in the EU Member States.

- The CPPNM, as amended in 2005, is the most important multilateral instrument that addresses nuclear security. At present, a few EU Member States have not yet completed the internal process that would enable the deposit of their instrument of ratification, acceptance or approval of the amendment.

- IAEA has an essential and central role in strengthening the international nuclear security framework. The IAEA's "Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Rev.5) document and related Nuclear Security Series documents are of particular value in implementing and maintaining Member States' national nuclear security regime.

- The IAEA's IPPAS missions are of special importance in providing to Member States an external assessment of their security regime and are considered as the reference for nuclear security evaluation for EU Member States with established or planned NPPs.

- Nuclear security and nuclear safety measures should be designed, implemented and managed in NPPs in a coherent and synergistic manner.

- It is important to implement and maintain a strong nuclear security culture. At the national level, all entities involved in nuclear security, private as well as public, should fully commit to enhance security culture and to maintain robust communication and coordination of activities. Human resource development through exercises and training could help build a strong nuclear security culture.

- Regarding cyber threats and the key roles of IC/ICT-systems in any NPP, cyber security has to be considered with great attention.

- Competent authorities should have a firm understanding of the potential consequences of an intentional aircraft crash on a NPP. Measures and procedures for timely warning and alerting the NPPs in case of identification of a RENEGADE-aircraft potentially threatening NPPs should be considered at the national level.

- Several neighbouring countries with borders to the EU and with existing or planned NPPs have shown interest in the work of AHGNS. In general these neighbouring countries have expressed positive interest in a continued exchange of views and cooperation with the EU Member States regarding nuclear security.

- It is recognised that exchange of information on certain aspects of nuclear security requires the protection of confidential information and therefore the setting up of conditions allowing to share such information.

7.2. Recommendations

Although the security of NPP's is a national responsibility, the AHGNS, on the basis of its main conclusions, proposes the following recommendations:

- Urge all EU Member States which have not yet done it to complete as soon as possible the internal process that would enable the deposit of their instrument of ratification, acceptance or approval of the 2005 Amendment to the CPPNM. This will also set a good example for neighbouring countries and bring closer the date for the Amendment to enter into force.

- Encourage the use of IAEA's services and the use and implementation of IAEA's publications of the Nuclear Security Series in the Member States` national practices.

- Highly encourage the use of IAEA's IPPAS missions on a regular basis in all EU Member States with NPPs. Security issues relating to cyber threat should be part of the missions. EU Member States hosting an IPPAS mission also send an important message to other countries to do similarly.

- Encourage the IAEA to share, at the international level, best practices identified through the different IPPAS missions, taking due account of confidentiality requirements. The implementation of such best practices should be promoted.

- Encourage regular cooperation among EU Member States and between them and the EU's neighbouring countries. The cross-border nature of any nuclear incident is a strong motivation for close cooperation and exchange of information between countries.

- Continue the work on nuclear security among EU Member States, also in line with Action RN. 19 of the EU CBRN Action Plan. The AHGNS is convinced that continued cooperation between the EU Member States, including appropriate information exchange, on nuclear security is of value, using the framework of existing groups at the EU level. ENSRA is considered as an important body for enhancing nuclear security. The AHGNS calls upon this association to welcome nuclear security regulators of all EU Member States and those of neighbouring countries.

ANNEX I : 32 GOOD PRACTICES IDENTIFIED BY AHGNS

A National legal and regulatory framework

1. Without prejudice to more detailed requirements, including those mentioned in subsequent description of good practices, the main issues that are addressed in the national legal and regulatory framework for nuclear security, as regards both the objectives to be achieved and the measures to be taken, are largely set out in the CPPNMNF art. 2A) and in the INFCIRC/225/Rev.5 para. 2.1 for the main objectives. As several security related issues may also be addressed in other legal and regulatory framework for nuclear safety, radiation protection, safeguards, non-proliferation and transport of nuclear material, the interfaces with these other regulatory frameworks should be clearly specified in the nuclear security one.

2. Given the role the CPPNMNF plays as a reference point for the national legal and regulatory framework for nuclear security, the entry into force of its amendment is an urgent priority. The most recent revision of the IAEA recommendations INFCIRC/225/Rev.5 is taken into account in reviewing and implementing the national nuclear security legal and regulatory framework.

3. The nuclear security regime is assessed on a continuing and ongoing basis in order to achieve continuous improvements. The formal reviews of the nuclear security framework are carried out by the normal legislative and regulatory processes. It is a function of new developments in the international nuclear security instruments and guidance and lessons learned from significant events or substantial changes in a threat definition or scenario. The procedures for these reviews, including frequency, triggering factors and deadlines, are set out in the legal and regulatory framework. The IPPAS missions are an important instrument in the review process. IRRS missions including a security module could be useful as well.

4. The nuclear security of NPPs is maintained under the conditions set out by the scenarios considered at the design stage. This therefore is taken into account at the level of both operator and public authorities, notably by ensuring the consistency of contingency plans with those developed under other legal and regulatory frameworks, e.g. emergency plans for civil protection. It is also advisable to assess whether or not there is a need for specific nuclear security contingency plans in case of natural disaster and to what extent the national legal and regulatory framework should demand these contingency plans in case of natural disasters.

5. As part of its tasks under the national nuclear security framework the State has to carry out the definition and evaluations of the threat to the NPPs, be it through the DBT or the threat assessments. For this purpose the IAEA implementing guide Nuclear Security Series No 10 [1] about the development, use and maintenance of the Design Basis Threat may be considered. Following this evaluation process the preparation of scenarios of the threats is essential. These scenarios incorporate generic elements that are not NPP-specific and correspond to the threats considered by the State in the DBT, as well as NPP-specific elements. In order to evaluate the effectiveness of the nuclear security measures the physical protection system should be regularly tested with the participation of competent authority, operator and all other relevant organisations and authorities. The physical protection systems should be regularly reviewed according to the results of the above tests and current assessment of the threat. Given their value for potential adversaries special attention is given to the confidentiality of information related to the DBT, resulting threat scenarios and subsequent evaluation of the nuclear security measures.

[1] IAEA Nuclear Security Series No. 10 Development, Use and Maintenance of the Design Basis Threat.

6. The regulations related to nuclear security take into consideration various categories of nuclear material through a graded approach. Without prejudice to more refined categorisation, e.g. reflecting radiological consequences following unauthorised removal or sabotage, attractiveness to terrorists, etc. or more stringent requirements to be set on a national basis, Annex II to the CPPNMNF and section 4 of INFCIRC/225 Rev. 5 provide a good basis for the categorisation of such material.

7. Regarding ways and means to effectively reduce insiders threat the national legal and regulatory framework foresees the screening of persons in order to assess their trustworthiness and determine, in a graded manner, the areas in the NPP and category of material and of information to which they may have access, with special attention to temporary personnel. Therefore, exchange of intelligence between governmental departments and the operator with a view to detect or prevent malevolent action is a good practice. This is associated with security awareness programs for staff and management on site. A valuable additional measure is the two-person rule for access to highly protected areas to prevent or detect insider acts.

8. Besides reporting obligations linked to radiological emergencies as foreseen under EURATOM legislation, e.g. the ECURIE mechanism and the IAEA Convention on Early Notification, the reporting of nuclear security incidents are addressed in the national response plan and in the contingency plans and can be organised as follows:

- at the national level the operator immediately reports security incidents to the competent authority and police, which in turn liaise with other relevant authorities, e.g. intelligence;

- at the international level the State notifies to relevant international organisations and other States, combining as appropriate various information exchange mechanisms as the incident evolves (e.g. from theft to radiological consequences). The provisions of the CPPNMNF art.5 provide useful guidance. Relevant information exchange mechanisms are the IAEA Illicit Trafficking Database (ITDB), the Malicious Acts Database (MAD) and, in the European Union context, the European Nuclear Security Regulators Association (ENSRA), the EUROPOL Bomb Data Bank and reporting and exchange information foreseen under the Chemical, Biological, Radiological, Nuclear Action Plan.

Reporting is organised so as to preserve the confidentiality of information.

9. The national legal framework qualifies acts such as the theft of nuclear materials, sabotage or other malicious acts affecting NPP, notably those listed in the CPPNMNF art. 7 as punishable offences and foresee sanctions for such acts.

B National Security Framework

10. Nuclear security responsibilities are set in the nuclear national security regime and depend on a country's administrative arrangements and institutional setting as well as on the extent of its nuclear sector. These bodies in principle cover operators/licensees, regulatory body and other competent authorities.

Within the nuclear security regime defined by the State, with its support in term of high-level response and prevention/detection and intelligence measures and on the basis of the threat evaluation (e.g. definition of DBT) carried out by the State the operator has the prime responsibility for the implementation of nuclear security measures notably structures, systems and procedures on site.

The allocation of responsibilities between the operator and the State is clearly defined as regards on response against threats within DBT and the necessary resources exist. In situations involving threat within and beyond the DBT additional intervention resources are available on a local and national level in order to complete forces and resources of nuclear security at operator level. Depending of the State organisation, contingency plans consistent with emergency plans are established to handle those situations (see also item 8).

Modalities for the coordination of the operator security resources, which could include private security companies, with public authorities resources are addressed by the national legal framework and in contingency plans.

11. The existence of validated nuclear security measures, for instance in the form of a site security plan, is a condition for the granting of license (or other authorising document) for the operation of any NPP before carrying out any activity using nuclear material. Detailed information on a confidential basis from the operator which includes a description of the physical protection system and a study showing its effectiveness is taken as a basis by the competent authority which could be the regulatory body.

12. Nuclear Security requirements are already taken into consideration at a very early stage in the life-cycle of any NPP when deciding whether to build it on a given site, on the basis of the DBT or the threat assessment and taking into account the possible vulnerabilities that any NPP may face from its installation on a particular site.

The implementation of nuclear security measures should be required already at the building stage on the construction site or at least before the commissioning stage. The implementation and test of the full set of measures should be completed prior to the placement of nuclear material on-site.

13. The effective independence of the regulatory body responsible for the implementation of the regulatory framework for the nuclear security of NPP from other bodies or authorities responsible for the promotion or use of nuclear energy is ensured. Means of this regulatory body in order to ensure its independence cover its status, legal power, competence and financial and human resources.[1]

14. On the basis of experience so far and noting the voluntary nature of Nuclear Security Advisory Services, which are the IAEA's main tool for helping States to assess their nuclear security needs, these Services provide a valuable basis assisting the States in formulating plans of action for improving nuclear security

15. The Defence in Depth approach is implemented at all stages - prevention, detection, delay and response - of the nuclear security system, through a combination of physical (e.g. barriers for restricted, protected and vital areas), personal (e.g. guards) and organisational (e.g. trustworthiness check, promotion of security culture) measures and the coordination of resources at operator and authorities level.

[1] See for example Art. 5 in Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations (OJ L 172, 2.7.2009, p. 18 – 22) or Fundamental Principle D, 2nd sentence in the Amendment to the Convention on the Physical Protection of Nuclear Material (GOV/INF/2005/10) to Convention on the Physical Protection of Nuclear Material (INFCIRC/274/Revision 1)

16. Determination of the nuclear security measures necessary to counter assessed threats that may affect any NPP starts at an early stage in its development, preferably not later than the design stage, taking into account that part of the analysis concerns factors that may be relevant to the whole nuclear sector. It is also important to consider that the threats can evolve at the different stages of development of the project (design and construction).

17. Reference laboratories are useful means to test components of nuclear security system for any NPP while noting that the evaluation of the nuclear security systems fully rests with the State and that such tests can also be carried out through performance-based tests and do not dispense from actual exercises.

18. Regarding threats connected with the Information and Communication Technology (ICT) security, given the global range of such threats and the key role of Information and Communication Technology (ICT) systems in NPP, a high priority is assigned to cyber security. Efforts engaged by the IAEA as well as the EU (in relation with critical infrastructures) are intensified.

Cyber threats are addressed in a DBT or specific threat assessment. Adequate cyber security measures are applied to all ICT and Instrumentation and Control (I&C) systems and processes, if the manipulation of these systems directly or indirectly can lead to a loss of safety functions.

Data transfer into safety systems may only be allowed in exceptional cases and if it is proven, that this data transfer cannot lead to a loss of safety functions. There is reporting of cyber attacks from NPPs to the national level, as appropriate.

C Design Basis Threat

19. The physical protection system of NPP is based on the State's current evaluation of the threat which is formalised through a threat assessment process and includes all the credible threats. The DBT approach is used for the threat of unauthorised removal of sensitive nuclear material inside NPPs and sabotage of NPPs and their nuclear material that has potentially high radiological consequences.

20. The list of participants that are involved in defining the DBT will vary according to the organisation of the national security regime, several experts from different organisations with expertise in the field of nuclear security work closely together and provide input to the definition of DBT. As a minimum one would expect that the competent authority, and State-level body in charge of intelligence, police and other institution which could have important information for defining DBT will be involved.

21. When defining the DBT a lot of important areas and factors are taken into consideration. It is very important to have credible information from intelligence and competent authority which is the background for description of technical and human capabilities of groups posing credible criminal or terrorist threats, geopolitical context and insider threats of the NPPs (see also IAEA Nuclear Security Series No. 10).

22. Given that DBT are usually defined over the medium term (regular) threat assessment is used to assess whether an earlier update of the DBT is justified before the planned formal review is carried out and additional measures are called for in the meantime. Additional evaluations of the vulnerability of different NPPs are worthwhile and provide a different perspective, additional threats not included in the DBT are considered relevant or technical development have occurred.

23. In order to enable the bodies responsible for the definition of the DBT to get the information required for to prepare and update the DBT all reliable national and international sources of information should be considered and the flow of information and the cooperation between the various participants in the national nuclear security regime is clearly arranged. There is a mechanism for the exchange and flow of information among various participants which guarantee the confidentiality, integrity and availability of information. Such mechanism also ensures that sensitive information is appropriately protected by using a national system of information classification.

24. The monitoring and analysis of threats concerning the physical protection system of NPPs is based on evaluation and analysis of information obtained from intelligence organisations, competent authority, state law enforcement, operators and open sources. All gathered information is evaluated for credibility and reliability. In particular the activities of groups which pose credible threats will be specifically monitored. The main responsibility concerning external threats is at the intelligence organisations which have appropriate methods, tools, technologies and experience in this field.

D Nuclear Security Culture

25. Nuclear security culture complements the concept of safety culture and is an essential component of the nuclear security of NPPs. Nuclear security culture is promoted at all levels. All organisations and individuals involved in nuclear security of NPPs are aware of the importance of nuclear security culture. The requirements of high Nuclear Security Culture can be stated in the national legal and regulatory framework. Nuclear security culture is defined as the assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions. In particular the following is included: beliefs and attitudes that credible threats exist and security is important; clear and understandable security policy; clear roles and responsibilities; performance measurement; involvement of management, training and qualification. Effective security culture is an important element in ensuring effective information security; operation and maintenance of security system; adequate determination of staff trustworthiness; quality assurance; feedback process; contingency plans and drills; self-assessment; interface with the regulator; coordination with off-site organisations (see also IAEA Nuclear Security Series No. 7.[1]).

[1] IAEA Nuclear Security Series No. 7 Nuclear Security Culture.

26. The regular maintenance and inspection of existing physical protection system of NPPs is a key component of the nuclear security and is supported by a strong management system and performed according to approved procedures and schedules to ensure that design requirements will not be compromised. The operator ensures that security systems remain effective in accordance with conditions set by the competent authority, report failures and take corrective measures. Regular inspections should be achieved by the competent authority which could be the regulatory body. Performance verification tests and exercises (such as force-on-force) are done regularly and could be used to assess the adequacy of physical protection system. Any detected failures are notified to the competent authority which could be the regulatory body.

27. Managers with particular responsibilities for the nuclear security of NPPs participate in trainings at the national or international level. The program of such trainings is to be based on credible scenarios of incidents or attacks and, in order to improve response adequacy, addresses coordination, including coordination between operator and authorities, and communication issues, including in an international context. IAEA training programs are valuable in this respect. Given that bodies in charge of intelligence gathering or law enforcement are normally cooperating with persons responsible for the nuclear security of NPPs be it at the stage of threat assessment or when providing additional response in case of breach of nuclear security they are consulted when formulating training programs or designing exercises. The training policy is described and approved by the appropriate competent authority.

They could combine table-top exercises to evaluate the nuclear security plan and system as a whole as well as field exercise, including force-on-force exercises.

28. In order to ensure the maintenance of effective nuclear security of NPPs international cooperation could contribute to sharing experience and best practice, facilitate recovery of nuclear material unlawfully removed from NPPs, disseminate information on theft or sabotage and enrich the information underlying threat assessments. Given confidentiality requirements practical arrangements may have to be set under bilateral agreements. The relevant provisions of the CPPNMNF [1] state how to organise such cooperation. The IAEA plays the key role in coordinating this coordination through international training courses, technical meetings, workshops, conferences, scientific visits and other international activities. It allows participants to share the experience and exchange best practices in the nuclear security field.

The ENSRA as the European forum for exchanges on nuclear security matters assures confidential exchange of information and mutual professional assistance to achieve a common approach of nuclear security practices within the EU Member States, recognising the continuing need for variation between Member States to reflect different national circumstances.

Preserving the confidentiality of sensitive information is one of the primary concerns regarding the exchange of information with other countries concerning potential terrorist attacks which threaten the security of NPPs.

[1] See: Art 5 in Convention on the Physical Protection of Nuclear Material (INFCIRC/274/Revision 1) and Amendment to the Convention on the Physical Protection of Nuclear Material (GOV/INF/2005/10).

As a form of cooperation among Member States and other players, international guidelines and training activities and recognised best practices are valuable when modernising nuclear security for nuclear materials and NPPs.

29. General rules for the classification, handling of and access to sensitive information are usually set at State level. If it is necessary the competent authority issues additional regulatory requirements and implementing guidelines. More detailed procedures on the protection of information on the functioning of NPPs and the storing of their nuclear material, especially as regards physical protection measures, can be defined at the NPP level

E Contingency Planning

30. The main components of plans of security and contingency at national level define the role and responsibilities of the State various response organisations, describes communication and coordination between participating organisations by security events, policy and concept of operations for the response.

Such plans include: off and on site planning, sector resilience planning, responsibilities of participating organisations (like operator, competent authority, police, crisis management authorities, etc.), response process and recovery, command, control and coordination structure (addressing allocation of responsibilities and rule for notification of events), communication protocols, technical support (including training programs), test and review procedures.

Such plans to cope with security incidents are adequately considered in the nuclear emergencies organisations and carried out in coordination with the nuclear off-site emergency plans.

31. While the list of participants in the national nuclear security regime is likely to vary according to the extent of the nuclear sector and to the organisation of the national security, responsible for preparing contingency plans in order to address nuclear security incidents, are likely to include operators, competent authority, authorities providing additional resources (on and off site response forces, counter terrorism, intelligence civil protection etc.).

32. Plans mentioned in item 31. prepared to deal with malevolent actions against NPPs include at least triggering criteria, communication procedures, cooperation/coordination among operator and public authorities, command structure, public awareness, interface with radiological emergency plan, technical support, training and testing, review and update, in close relation with other national legal regulations.

ANNEX II : ACRONYMS

AHGNS	Ad Hoc Group on Nuclear Security
CBRN	Chemical, Biological, Radiological, Nuclear
CPPNM	Convention on the Physical Protection of Nuclear Material
CPPNMNF	Convention on the Physical Protection of Nuclear Material and Nuclear Facilities
DBT	Design Basis Threat
ECURIE	European Community Urgent Radiological Information Exchange
ENSRA	European Nuclear Security Regulators Association
EURATOM	European Atomic Energy Community
IAEA	International Atomic Energy Agency
ICT	Information and Communication Technologies
IC	Instrumentation and Control systems
IPPAS	International Physical Protection Advisory Service
IRRS	Integrated Regulatory Review Service
ITDB	Illicit Trafficking Database
MAD	Malicious Acts Database
NPP(s)	Nuclear Power Plant(s)
NSS	Nuclear Security Summit

ANNEX III : REFERENCE DOCUMENTS

1. Convention on the Physical Protection of Nuclear Material (INFCIRC/274/Revision 1) and Amendment to the Convention on the Physical Protection of Nuclear Material (GOV/INF/2005/10)
2. IAEA Nuclear Security Series, including:
   - 2a IAEA Nuclear Security Series No. 9 Security in the Transport of Radioactive Material
   - 2b IAEA Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)
   - 2c IAEA Nuclear Security Series No. 14 Nuclear Security Recommendations on Radioactive Material and Associated Facilities
   - 2d IAEA Nuclear Security Series No. 17 Computer Security at Nuclear Facilities.
3. Convention on Early Notification of a Nuclear Accident
4. Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations (OJ L 172, 2.7.2009, p. 18–22)
5. IAEA Safety Glossary

ANNEX IV : GLOSSARY[1]

Competent authority: governmental organisation(s) or institution(s) that has (have) been designated by a State to carry out one or more nuclear security functions.

Contingency plan: predefined sets of actions for response to unauthorised acts indicative of attempted *unauthorised removal* or *sabotage,* including *threats* thereof, designed to effectively counter such acts.

Defence in depth: the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised.

Design basis threat: the attributes and characteristics of potential *insider* and/or external adversaries, who might attempt *unauthorised removal* or *sabotage,* against which a *physical protection system* is designed and evaluated.

Emergency plan: A description of the objectives, policy and concept of operations for the response to an emergency and of the structure, authorities and responsibilities for a systematic, coordinated and effective response. The emergency plan serves as the basis for the development of other plans, procedures and checklists. [Ref. doc. 5]

Force-on-force exercise: a *performance test* of the *physical protection system* that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the *threat* or the *design basis threat.*

Graded approach: the application of *physical protection measures* proportional to the potential consequences of a *malicious act.*

Guard: a person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.

[1] Unless otherwise mentioned all definitions come from Ref. document 2.b.

Insider: one or more individuals with authorised access to *nuclear facilities* or *nuclear material* in *transport* who could attempt *unauthorised removal* or *sabotage,* or who could aid an external adversary to do so.

Malicious act: an act or attempt of *unauthorised removal* or *sabotage.*

Nuclear material: *nuclear material* is defined to be any material that is either special fissionable material or source material as defined in Article XX of the IAEA Statute [Ref. doc. 5].

(Nuclear) security: the prevention and detection of and response to theft, *sabotage*, unauthorised access, illegal transfer or other *malicious acts* involving nuclear material, other radioactive substances or their associated facilities (footnote 1 from Ref. doc. 2a).

Nuclear security culture: the assembly of characteristics, attitudes and behaviours of individuals, organisations and institutions which serves as means to support, enhance and sustain nuclear security.

Nuclear security measures: measures intended to prevent a *threat* from completing a *malicious act* to *detect* or respond to *nuclear security events*[Ref. doc. 2c] .

Nuclear security regime: a regime comprised of:

- the legislative and regulatory framework and administrative systems and measures governing the nuclear security of nuclear material, other radioactive material, associated facilities, and associated activities,
- the institutions and organisations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;
- nuclear security systems and nuclear security measures for the prevention of, detection of, and response to, nuclear security events [Ref. doc. 2c].

Nuclear security system: an integrated set of *nuclear security measures* [Ref. doc. 2c].

Operator: any person, organisation, or government entity licensed or authorised to undertake the operation of a *nuclear facility.*

Performance testing: testing of the *physical protection measures* and the *physical protection system* to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements.

Physical Protection measures: the personnel, procedures, and equipment that constitute a *physical protection system.*

Physical protection system: an integrated set *of physical protection measures* intended to prevent the completion of a *malicious act.*

Regulatory body: one or more authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing authorisations [Ref. doc. 2c].

Response forces: persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted *unauthorised removal* or an act of *sabotage.*

Sabotage: any deliberate act directed against a *nuclear facility* or *nuclear material* in use, storage or *transport* which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.

Threat: a person or group of persons with motivation, intention and capability to commit a *malicious act.*

Threat assessment: an evaluation of the *threats* — based on available intelligence, law enforcement, and open source information — that describes the motivations, intentions, and capabilities of these *threats.*

Two person rule: a procedure that requires at least two authorised and knowledgeable persons to be present to verify that activities involving *nuclear material* and *nuclear facilities* are authorised in order to detect access or actions that are unauthorised.

Unauthorised removal: the theft or other unlawful taking of *nuclear material.*

Vital area: area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences.

_____