

*INTERNATIONAL PHYSICAL PROTECTION
ADVISORY SERVICE (IPPAS)*



INTERNATIONAL ATOMIC ENERGY
AGENCY (IAEA)

Follow-up Mission Report: The Netherlands

23 January–3 February 2012

Prepared for the Inspector General for Human Environment and Transport,
The Kingdom of the Netherlands.

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

COPY 3 OF 3
HIGHLY CONFIDENTIAL:
TRANSMISSION AGAINST
SIGNATURE ONLY

HIGHLY CONFIDENTIAL:
TRANSMISSION AGAINST
SIGNATURE ONLY

*This report was prepared by a team representing the
International Atomic Energy Agency, Vienna, Austria.*

**HIGHLY CONFIDENTIAL:
TRANSMISSION AGAINST
SIGNATURE ONLY**

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AT	arrest team
BAC	central alarm station located at IIFR
BIP	security information package
BRK-93	<i>Security Guidelines for Nuclear Plants</i> (Netherlands)
BRTNM	Netherlands nuclear material transport requirements
CAS	central alarm station
CCS	central control station
CCTV	closed circuit television
CMP	central alarm post (Petten)
CNBS	Coordinator for Nuclear Security and Safeguards
COVRA	Central Organization for Radioactive Waste
CPPNM	<i>Convention on the Physical Protection of Nuclear Material</i>
CPPNMA	<i>2005 Amendment to the CPPNM</i>
DBT	design basis threat
DSI	police unit special interventions (special forces)
EBO	external security plan
ECN	Energy Research Centre of the Netherlands
EL&I	Ministry of Economic Affairs, Agriculture and Innovation
EPZ	Electricity Production Company Southwest of the Netherlands
ET NL	Enrichment Technology Netherlands
FTE	full-time equivalent

**HIGHLY CONFIDENTIAL:
TRANSMISSION AGAINST
SIGNATURE ONLY**

G4S	(company name: not an acronym)
HABOG	high radioactive treatment and storage building
HCL	hot cell laboratory
HEU	high enriched uranium
HFR	high flux reactor
IBO	internal security plan
IDS	intrusion detection system
ILT	Inspectorate for Human Environment and Transport
IPPAS	International Physical Protection Advisory Service
IPS	intrusion prevention system
ISAC-Nuclear	
ISO	International Organization for Standardization
IT	information technology
JRC	Joint Research Centre (of the European Commission)
KFD	Department for Safety, Security and Safeguards
kWth	kilowatt (thermal)
LEU	low enriched uranium
LFR	low flux reactor
MPF	molybdenum production facility
MR	<i>Nuclear Energy Plants and Fissile Material Protection Regulation</i>
MTR-2	material test reactor cask
MWe	megawatt (electric)
MWth	megawatt (thermal)
NBS	Nuclear Security and Safeguards division

NMAC	nuclear material accountancy and control
NPP	nuclear power plant
NRG	Nuclear Research and Consultancy Group
NSS	<i>Nuclear Security Series</i>
PALLAS	(proposed research reactor; not an acronym)
PIR	passive infrared
PPS	physical protection system
QSE	Quality, Safety, and Environment [Department]
RID	Reactor Institute Delft
SAS	substances, waste and radiation
SMS	security management system
SNB	Radiation Protection, Nuclear Safety and Biosafety division
SP	centrifuge plant
TRANSRAD	(company name, not an acronym)
UNL	URENCO Netherlands BV
URENCO	(company name; not an acronym)
VLAN	virtual local area network
VROM	Inspectorate of Housing, Spatial Planning and the Environment
WAN	wide-area network
WINS	World Institute of Nuclear Security
WSF	waste storage facility

**HIGHLY CONFIDENTIAL:
TRANSMISSION AGAINST
SIGNATURE ONLY**

CONTENTS

ABREVIATIONS	3
I. SUMMARY	9
II. INTRODUCTION.....	12
III. NATIONAL LEVEL LEGISLATIVE AND REGULATORY FRAMEWORK	14
A. Response to Previous IPPAS Mission Recommendations and Suggestions	14
1. Introduction	14
2. IPPAS 2005	14
3. IPPAS 2008	18
4. IPPAS 2009	20
B. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5 and CPPNMA)	20
C. Computer Security Provisions at State Level	24
1. Legal and Regulatory Framework for Computer Security	24
2. Design Basis Threat (DBT).....	25
3. Coordination.....	25
IV. FACILITY LEVEL IMPLEMENTATION	26
A. Borssele Nuclear Power Plant	27
1. Overview	27
2. Response to Previous IPPAS Mission Recommendations and Suggestions	28
3. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5).....	34
4. Summary	38
B. COVRA	39
1. Overview	39
2. Response to Previous IPPAS Mission Recommendations and Suggestions	39
3. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5).....	42
4. Summary	44
C. Petten.....	46
1. Overview	46
2. Response to Previous IPPAS Mission Recommendations and Suggestions	47
3. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5).....	51
4. Summary	54

D. Reactor Institute Delft	55
1. Overview	55
2. Response to Previous IPPAS Mission Recommendations and Suggestions	55
3. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5).....	57
4. Summary	60
E. URENCO Netherlands	61
1. Overview	61
2. Response to Previous IPPAS Mission Recommendations and Suggestions	61
3. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5).....	67
4. Summary	70
V. ACKNOWLEDGEMENTS	71
Appendix I: Synopsis of Recommendations, Suggestions and Good Practices	72
Appendix II: IPPAS Team Composition	77

IPPAS FOLLOW-UP MISSION REPORT: NETHERLANDS

I. SUMMARY

This report presents the results of the International Physical Protection Advisory Service (IPPAS) follow-up mission conducted by the IAEA (from 23 January to 3 February 2012) at the request of the Kingdom of the Netherlands through the Inspectorate of Housing, Spatial Planning and the Environment (VROM-Inspection). VROM-Inspection has recently been reorganized and incorporated into the Inspectorate for Human Environment and Transport (ILT) of the Ministry of Infrastructure and the Environment.

The Netherlands was among the first three countries in Western Europe to invite an IPPAS mission and the first in Western Europe to invite a follow-up mission. Three IPPAS missions have now been conducted in the Netherlands, in addition to this follow-up mission. The first mission, in December 2005, comprised a national level review and a review of physical protection at the Borssele nuclear power plant (NPP); the second, in September 2008, reviewed physical protection at four nuclear facilities: the Central Organization for Radioactive Waste (COVRA), the Reactor Institute Delft (RID), the decommissioned Dodewaard NPP, and the Petten Research Centre; and the third, in June 2009, reviewed physical protection of the URENCO Netherlands BV (UNL) site.

The primary objective of the follow-up mission was to review the implementation of recommendations and suggestions provided at State and facility level during the previous three IPPAS missions using *INFCIRC/225/Rev.4* as the main reference document. The second objective was to review the current status of the State's physical protection regime of nuclear material and nuclear facilities — including the physical protection measures in place at nuclear facilities — and to compare this current status with the requirements recommended by *INFCIRC/225/Rev.5* and with the provisions of the *2005 Amendment to the CPPNM (CPPNMA)*. At the request of the Netherlands, the IPPAS team also reviewed the measures taken by State authorities and facility operators to ensure the security of computer systems used for security purposes or as part of control systems for other vitally important processes at nuclear facilities.

A team of seven international experts — representing five Member States and the IAEA, and with a variety of expertise in different areas related to nuclear security and physical protection — conducted the review. The team interacted with personnel representing the governmental policy and regulatory organizations of the Netherlands and also with key management and staff of the five nuclear facilities (Borssele NPP, UNL, RID, COVRA and the Petten Research Centre) which were visited during the mission.

It was noted that nuclear security within the Netherlands is currently in transition, with significant changes in the structure of nuclear-related regulatory organizations. The new regulatory requirements on physical protection, which were approved by the Minister of Economic Affairs, Agriculture, and Innovation at the end of 2010, include a change in principle from a prescriptive, compliance-based approach to a performance-based approach. The new regulations will require operators and regulators to change their approach to nuclear security.

The IPPAS team recognized that significant efforts have been made by the State authorities and facility operators to implement the recommendations of previous IPPAS missions and that the

majority of these recommendations have now either been implemented or are being implemented. At the State level, the main developments include the following:

- An increase of staff at NBS and the establishment and implementation of an extensive inspection programme.
- Promulgation by the Minister of Economic Affairs, Agriculture and Innovation (in December 2010) of the new Nuclear Energy Plants and *Fissile Material Protection Regulation* (hereafter referred to as MR), which is in accordance with *INFCIRC/225/Rev.4* and with some provisions of *INFCIRC/225/Rev.5*;
- Development and issuance by the Minister of Economic Affairs, Agriculture and Innovation (in March 2011) of the design basis threat (DBT) (which has also been provided to facilities operators to implement effective physical protection measures against it). The DBT was also approved by Ministers at the Ministry for the Interior and the Ministry of Justice;
- In April 2011 the Netherlands announced acceptance of the 2005 *CPPNMA* (national legislation was reviewed and amended to ensure compliance);
- Promulgation by the Minister of Interior (in January 2012) of new vetting requirement for nuclear industry employees.

Across the board, nuclear facilities within the Netherlands are on a path of improvement with regard to nuclear security. Significant implementation of the recommendations and suggestions made by previous missions in respect of nuclear facilities has been achieved through additional or new organizational, procedural and technical physical protection measures.

At the Borssele NPP in particular, the ongoing large scale upgrades of the physical protection system (PPS) are based on the site's new conceptual approach (including the concerted action of security, safety, plant operation personnel and off-site response forces) and will be completed shortly. Extensive joint exercises have been used to test and confirm the effectiveness of the PPS. The development of this concept for physical protection and its implementation are to be commended. Furthermore, the IPPAS team believes that the application of such an approach at all other high-risk nuclear facilities which contain Category I nuclear material or which pose a potential radiological sabotage risk exceeding State-defined thresholds, would be of great benefit to nuclear security in the Netherlands.

It is important to note that despite the efforts made to improve the PPS at the Petten Research Centre, the site does not yet meet international recommendations defined in *INFCIRC/225/Rev.4* and falls short of national regulatory requirements. Additional urgent action should be taken to mitigate potential vulnerabilities and to ensure effective physical protection of the inventories of nuclear material held at this site. Emphasis should be placed on removing the HEU from the LFR.

A total of 14 new recommendations and 37 new suggestions have been made and 6 good practices have been identified. These are all listed at Appendix I. Key recommendations relate to the establishment of the effective independence of the competent authority (defined as the policy body and the regulator), further development of physical protection requirements and guidance, and computer security. Other recommendations relate to improvement of physical protection measures at nuclear facilities. Good practices include implementation of physical protection concepts and computer security measures at the Borssele NPP, and coordination among the information security managers across all nuclear sites.

The current Security and Safeguards Coordinator (CNBS) has played a pivotal role in establishing the momentum for change. Replacing him when he retires at the end of 2012 with a competent and experienced successor will be an essential step in consolidating the improvements which have been made so far and sustaining the current trend of improvement.

The IPPAS team noted the interest expressed by the Dutch with regard to building a second NPP at Borssele and constructing another research reactor (PALLAS) at Petten. While the team accepts that neither project is certain at this point, they recommend early involvement of the competent authority in the design of both the plants to ensure that security requirements are incorporated from the start. Early inclusion of essential security planning will reduce the need to retrofit security measures at a later stage in construction, and probably at greater cost. Security at these new facilities should be designed with the view to planning for the long-term and the likely operational life of both plants.

The IPPAS team concludes that a firmly grounded physical protection regime exists within the Netherlands and appropriate physical protection measures are in place or are being developed at nuclear facilities. The overall conclusion of the review indicates that the state of physical protection — from policy to implementation — within the Dutch nuclear industry in general is significantly improving. The recommendations and suggestions included in this report are intended to serve as a guide to assist the Netherlands in applying a process of continuous improvement in nuclear security, and aligning it further with international legal instruments and *INFCIRC/225/Rev.5*. The identified good practices might assist other Member States in strengthening their nuclear security regimes

This report, containing the results of the review, is for the exclusive use of the Government of The Kingdom of the Netherlands who may share the report as it sees fit. Measures were taken to protect the confidentiality of the report and the underlying information.

II. INTRODUCTION

The IPPAS programme, initiated in 1995, is a fundamental part of the IAEA efforts to assist Member States to establish and maintain an effective physical protection regime for protection against the theft of nuclear material and the sabotage of nuclear facilities and material. The IPPAS programme is offered to assist Member States, upon request, with an appraisal of their State physical protection regime. This appraisal includes a national-level review of the legal and regulatory framework, and the measures and procedures in place to execute that framework at facilities and during transport. Since 1996, 53 IPPAS missions have been conducted in 37 countries.

This report presents the results of the IPPAS follow-up mission conducted from 23 January to 3 February 2012 for the Inspectorate for Human Environment and Transport (ILT) of the Ministry of Infrastructure and the Environment of the Netherlands.

The Netherlands was among the first three countries in Western Europe to invite an IPPAS mission. Three IPPAS missions have been conducted in the Netherlands in the past: the first mission, in December 2005, comprised a national level review and a review of physical protection at Borssele nuclear power plant (NPP). The second, in September 2008, reviewed physical protection at four nuclear facilities: the Central Organization for Radioactive Waste (COVRA), the Reactor Institute Delft (RID), the decommissioned Dodewaard NPP, and the Petten Research Centre. The third, in June 2009, reviewed physical protection of the URENCO Netherlands BV (UNL) site.

The Netherlands was the first country in Western Europe to invite an IPPAS follow-up mission. The request to conduct a follow-up IPPAS mission was received on 23 March 2011 from VROM-Inspection (now incorporated into the structure of ILT). A preparatory meeting for this mission was held on 30–31 August 2011 and the mission was conducted during the period 23 January–3 February 2012.

The objectives of the IPPAS mission were to:

- review the implementation of the recommendations and suggestions made during the previous three IPPAS mission conducted in the Netherlands (using *INFCIRC/225/Rev.4* and *Physical Protection Objectives and Fundamental Principles* as reference documents);
- review the current status of the physical protection regime of nuclear material and nuclear facilities in the Netherlands and its compliance with the provisions of the 2005 *Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNMA)*;
- compare current practices on physical protection of nuclear material and nuclear facilities in the Netherlands, including computer security in particular, with guidance provided in IAEA Nuclear Security Series (NSS) No.13, *Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities* (also *INFCIRC/225/Rev.5*, as further referred to in this report), and in other NSS guidance.

Six physical protection experts (including an IAEA technical officer) and a computer security expert participated in this IPPAS mission team (details are at Appendix II). All these specialists have broad experience in physical protection system design, implementation, regulatory oversight, and nuclear legislation. Three of the experts had participated in at least one previous IPPAS mission to the Netherlands and the team leader, Mr Joe Sandoval, had participated in all of them.

The IPPAS team reviewed progress against the recommendations and suggestions made during the missions conducted in 2005, 2008 and 2009. They recorded their observations based on the recommendations in *INFCIRC/225/Rev.4* and developed new recommendations and suggestions using *INFCIRC/225/Rev.5* as the basis.

The team gathered information on the current legal and regulatory structure through interviews with government officials representing the Ministry of Economic Affairs, Agriculture and Innovation, and the Department for Safety, Security and Safeguards (KFD) of ILT. Facility visits were made to all operating nuclear facilities including: Borssele NPP, RID, COVRA, URENCO Netherlands BV (UNL) and Petten Research Centre. Dodewaard NPP was not visited because it is decommissioning and no longer has nuclear material at the site.

The team observed the implementation of physical protection practices and held discussions with personnel of visited facilities. At Borssele NPP, the IPPAS team was also able to observe a security exercise, which provided an opportunity to gather additional information on response to security incidents. Meetings with Government officials and facility staff, as well as visits to the facilities, provided opportunities for informal exchange of information on physical protection practices used in other countries and for discussion of the technical aspects of implementing physical protection systems.

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

III. NATIONAL LEVEL LEGISLATIVE AND REGULATORY FRAMEWORK

A. Response to Previous IPPAS Mission Recommendations and Suggestions

1. Introduction

Since the last IPPAS mission to the Netherlands in June 2009, the State has embarked upon a significant revision of the legislative and regulatory framework underpinning security in the nuclear sector. The Netherlands introduced a new set of regulations for nuclear security (*Nuclear Energy Plants and Fissile Material Protection Regulation*, hereafter MR) in December 2010; established a national design basis threat in March 2011; and also accepted the 2005 CPPNMA in April 2011, following the appropriate adjustment in national legislation. This adjustment included amendment of the *Nuclear Energy Act* to explicitly recognize nuclear security. During the 2012 IPPAS follow-up mission, the IPPAS team understood that a revised policy had been agreed upon with regard to the screening (personnel security/vetting) of personnel employed in the nuclear sector with access to nuclear material or sensitive nuclear information. At the same time that these legislative and regulatory developments were occurring, a reorganization of ministerial responsibilities and ministries enabled the separation of the policy and the inspection functions relating to security in the nuclear sector. Additional resources have been authorized to enable an increase in the numbers of the Security and Safeguards Coordinator's (CNBS's) inspection staff and additional staff have now been recruited. These are welcome developments and reflect a sustained commitment by the Dutch Government to respond effectively and proportionately to the general threat to the use of nuclear technology for peaceful purposes. It also puts the Netherlands in a good position to host the Nuclear Security Summit in 2014.

This commitment has in turn been reflected in the response noted by the 2012 IPPAS mission to the 12 State-level recommendations and 10 State-level suggestions made during the 2005, 2008 and 2009 IPPAS missions. All these recommendations have either been met or are in the process of being implemented. One recommendation cannot be implemented for wider legal reasons but alternative measures to meet their intent are now in place. All State-level suggestions have also either been met or are in the process of being implemented. The details of each recommendation and suggestion and the response to each are described below.

2. IPPAS 2005

Recommendations to strengthen Nuclear Policy and Regulations:

Recommendation 1: Determine if the staff of the KFD/NBS and SAS/SNB are sufficient to meet all the requirements of their respective areas of responsibilities.

Response: Since 2005, the policy and inspection functions have been separated and staff numbers in both areas have doubled. This separation has been accompanied by a rationalization of roles and responsibilities within NBS with the aim of developing and maintaining a clear focus on core roles associated with the regulation of nuclear security.

As well as the CNBS, the NBS now has three full time inspectors dedicated to providing security oversight in the nuclear sector, and a fourth inspector dealing with the security of radioactive sources.

With the developing focus on core roles, the CNBS believed that he was now in a much better position to regulate security in the nuclear sector.

The IPPAS team notes that the CNBS will retire at the end of 2012 and that it will be a significant challenge to select a successor with an appropriate level of skills, knowledge and experience to maintain the current level of service.

The IPPAS team welcomed the fact that safety, security, and safeguards are now all in the same organization and that positive efforts are being made to promote greater synergy between the three regulatory disciplines. This is an example of good practice.

Good Practice [New] 1: Safety, security, and safeguards are now in the same organization, KFD/NBS, thereby offering greater opportunities to promote greater synergies between the three regulatory disciplines.

Recommendation 1 has now been met.

Recommendation 2: Develop a design basis threat (DBT) which defines baseline physical protection objectives.

Response: The Netherlands is undertaking a significant and comprehensive overhaul of its regulatory framework and these comments on Recommendation 2 are made in the knowledge that some important policy documents have only recently been introduced or revised. The IPPAS team accepts that it takes time for all stakeholders to become fully familiar with the content of such documents.

Following consultations between the regulator, the sites and other stakeholders, a working document on national DBT was approved by the Minister of VROM in 2008. The DBT was then formally brought into force by the Ministry of Economic Affairs, Agriculture, and Innovation in March 2011.

Not all sites appeared to be fully familiar with the detail contained within the national DBT and, equally, there seemed to be limited understanding of how the malicious capabilities described in the document should inform the planning assumptions against which a site's security plan should be framed. The IPPAS team is confident that this level of understanding will develop and improve with time, but promoting greater understanding should be a priority for NBS.

New Suggestion 1: Within the constraints of the document's protective marking, the State and the sites could collaborate to develop greater clarity with regard to the content of the national DBT and the importance of the DBT in providing the basis for the assumptions underpinning a site's security plan.

Recommendation 3: Establish legislation to give appropriate authority to guard force personnel in order to improve their ability to protect the plant against the defined DBT.

Response: In the Netherlands, the law does not allow contract guards to use any form of physical restraint or non-lethal force which remain the prerogative of the law enforcement agencies acting on behalf of the State. The police, who can request the deployment of special forces, initially lead and provide the off-site response, which is coordinated through the EBO process. Sites assess delay times on the basis of their knowledge of the robustness and resilience of their facilities, compare these with response force times, and ensure that delay exceeds response time. In addition, sites take measures to mitigate the consequences of a sabotage event.

The IPPAS team saw clear evidence of a close working relationship between security staff and local law enforcement agencies at two of the sites visited, and noted the formal agreements underpinning the response arrangements and the clear commitment to exercise such plans.

This recommendation has been met.

Recommendation 4: Update nuclear security regulations, defined in BRK-93 to current guidelines in INFCIRC/225.

Response: On 7 December 2010, Ministers approved new regulations for nuclear security (MR) and all sites were expected to comply with the new regulations within 12 months from 1 January 2011. Two sites (Research Centre Petten and RID) were unable to meet this deadline and were given an additional month (to 31 January 2012) in which to complete their preparations to comply. Currently both BRK-93 and the MR are in effect. The plan is to eventually remove BRK-93 from the licences and withdraw it. However, there are still a few key provisions in BRK-93 and the existing licences which need to be included in the MR.

This recommendation is being implemented.

New Suggestion 2: The State might consider comparing BRK-93 and the current version of the MR, in order to identify any key provisions which are not yet included in the MR, and including applicable provisions in the future updated version of the MR. These provisions might include, for example, reporting to the CNBS.

Recommendation 5: Update the BRTNM, written in 1975, which dictates the requirements for the protection of nuclear material during transport, based on the guidelines in *INFCIRC/225* and the *Convention on the Physical Protection of Nuclear Material (INFCIRC/274)*, as amended from time to time.

Response: See comment on Recommendation 4 above: the new regulations will apply equally to the regulation of security associated with nuclear transport operations.

This recommendation has been met.

Recommendations to improve the Nuclear Facility and Transport Regulatory Inspection and Evaluation Programme

Recommendation 6: The effectiveness of the current methodology used to evaluate physical security systems does not appear to adequately assess the effectiveness of physical protection systems at nuclear facilities. It should be re-evaluated for adequacy by an independent body.

Response: The State has now adopted a performance-based approach, based on a defined DBT. The IPPAS team noted that the organizational changes described in the comments on Recommendation 1 above have complemented the introduction of new regulations, a robust inspection programme and a series of force-on-force exercises at sites. The numbers of inspectors have also been increased and they now produce inspection reports after each inspection. Reports are in two parts: the first part is an open source document to comply with the Dutch licensing system and the second is protectively marked for the exclusive use of the site management.

The recommendation has now been met.

Recommendation with regard to implementing Nuclear Security Fundamental Principle F — Development and Maintenance of a Security Culture

Recommendation 7: A formal security awareness programme should be developed to provide ongoing education to all personnel on the importance of effective physical protection measures for the protection of nuclear facilities and nuclear material and be trained in their implementation as appropriate.

Response: The IPPAS team noted that NBS had run a pilot workshop in 2011 on raising security awareness aimed at Chief Executive Officers. This pilot had been regarded as a success. The new MR also place a requirement on sites to describe measures to improve and promote security awareness and there was clear evidence at sites that this requirement was being implemented.

This recommendation has been met.

Recommendation 8: Re-evaluate the classification of information under protection to ensure that the information protection programme limits the potential for unauthorized disclosure that would compromise the physical protection of nuclear material, nuclear facilities, and nuclear material during transport.

Response: The IPPAS team noted that changes have been introduced which now prevent the routine release of sensitive nuclear information. Licence conditions identify sensitive nuclear information which requires a protective marking and authorizes the sharing of such information with those who need to know, including the police and other off-site responders. The CNBS is the authority for prescribing the protective marking that should be applied.

This recommendation has been met.

Suggestions

Suggestion 1: Re-evaluate the coordination between security and safety personnel during the transition from a security event to a radiation emergency event to include the transition of control from the police authority to the emergency response centre.

Response: This has been exercised on at least one occasion, at Borssele NPP, and showed areas that require further development. Ongoing activities, if sustained, will address this suggestion.

This suggestion is being implemented.

Suggestion 2: Establish better coordination on physical protection between countries during international transports, e.g. information on threats, levels of protection, emergency plans.

Response: The Netherlands conduct the majority of their international transport operations with Belgium and with France and all three countries are committed to reaching an agreement in line with *INFCIRC/225/Rev.5*. Similarly, the IPPAS team noted that a consignment of vitrified residue delivered to COVRA from the UK in 2010 was subject to a detailed planning process which involved all States and agencies affected by the move.

This suggestion has been met.

Suggestion 3: Review and, if necessary, clarify the role of the police during transportation.

Response: The IPPAS team noted that a draft agreement between NBS and the Dutch police with regard to the protection of nuclear transports has been prepared. The agreement is awaiting formal sign-off by the Minister of Economic Affairs, Agriculture and Innovation, but its requirements are being applied now.

This suggestion has been met.

Suggestion 4: Broaden the exposure of KFD (NBS) and SAS/SNB in physical protection; consult with regulators of other State parties; participate in international PPS workshops.

Response: In the past three years, the international profile of NBS has been raised. The Netherlands has hosted the annual meeting of the European Nuclear Security Regulators Association and it has enabled and supported IAEA-sponsored nuclear security Professional Development Courses at Delft. The Security and Safeguards Coordinator has played an important role in supporting IAEA activities, including playing a prominent role in coordinating European input to *INFCIRC/225/Rev.5* and leading an IPPAS mission to the UK in 2011.

This suggestion has been met.

Suggestion 5: Ensure that compliance inspections conducted by a competent authority are independent from the licensee.

Response: At present, the Ministry of Economic Affairs, Agriculture and Innovation (EL&I) is responsible for granting licences for the use, storage and processing of nuclear material. NBS reports to the Inspectorate of the Environment and Transport within the Ministry of Infrastructure and the Environment, and is responsible for nuclear security inspections at the sites. NBS also advises EL&I on major changes on security of nuclear plants and has the authority to approve both minor modifications and urgent measures prompted, for example, by a change in the threat.

The IPPAS team noted that this structure guarantees the independence of the inspection process from the licensees and that NBS reports directly to the Minister at EL&I.

The IPPAS team noted that there has been a substantial improvement in the NBS inspection programme. The team was briefed on the annual inspection programme for 2012, which included a substantial number of announced and unannounced inspections to the different sites. However, it seems that there are insufficient specific written procedures to support the programme. The NBS should consider whether to establish such procedures, describing the scope of the inspection process in different areas of the security system, and also the size of samples that should be covered in each area.

This suggestion has been met.

New Suggestion 3: The NBS could consider establishing inspection procedures that cover the entire inspection process, including the scope of the inspection, the process, and the size of samples that should be covered.

3. IPPAS 2008

Recommendation

Recommendation 1: The State should define requirements for the physical protection in transport depending on the associated consequences of either unauthorized removal of nuclear material or sabotage.

Response: The IPPAS team noted that the new MR includes measures to protect the transport of nuclear material.

This recommendation has been met.

Suggestions

Suggestion 1: VROM should consider using existing and emerging recommendations for the protection of radioactive sources to develop national-level requirements for the categorization and protection of sources.

Response: The IPPAS team noted that new regulations for the protection of radioactive sources¹, including categorization, were being prepared and were expected to come into force in 2012. These new regulations are based on the recommendations of the *Code of Conduct on the Safety and Security of Radioactive Sources*, the *IAEA Implementing Guide for the Security of Radioactive Sources*, and *NSS No.14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities*. The process of preparing the draft regulations had included a workshop for industry and hospitals, sponsored by the World Institute of Nuclear Security (WINS) and was also supported by the Dutch Society for Radiological Protection.

This suggestion has been met.

Suggestion 2: VROM should consider providing guidance for implementing the DBT when it becomes a regulatory requirement.

Response: NBS has assured the IPPAS team that the new national DBT defines an adversary's malicious capabilities and that judgments on how to counter such capabilities take account of the intrinsic delay associated with the physical protection measures at a site. NBS have yet to produce guidance on implementation due to resource constraints, but this remains a priority for the regulator.

This suggestion is still being implemented.

Suggestion 3: VROM should consider revising the policy for the protection of sensitive transport information.

Response: This suggestion has been adopted and implemented through the new MR.

This suggestion has been met.

Suggestion 4: The policy for transparency of transports could be reviewed to ensure that this policy does not introduce security vulnerability.

Response: The IPPAS team noted that NBS has sought legal advice with regard to the CNBS's mandate for direct access to the Minister of Economic Affairs, Agriculture and Innovation to provide the Minister with advice on what information can be released. Clarifying this access will allow the Security and Safeguards Coordinator to act in a timely manner to prevent unnecessary disclosure.

This suggestion is being implemented.

¹ MR Beveiliging van radioactieve stoffen

4. IPPAS 2009

Recommendations

Recommendation 1: The State should issue the revised BRK-93 as soon as practicable in order to ensure compliance with the recommendations in *INFCIRC/225/Rev.4* giving consideration to ongoing work to revise and publish *INFCIRC/225/Rev.5*.

Response: See response to 2005 State-level Recommendation 4, and New Suggestion 2.

This recommendation is being implemented.

Recommendation 2: The State should develop and formally issue a DBT from an evaluation of the threat of unauthorized removal of nuclear material and the sabotage of nuclear material and nuclear facilities.

Response: Following consultations between the regulator, the sites and other stakeholders, a working document on a national DBT was approved by the Minister of VROM in 2008. The DBT was then formally brought into force by the Ministry of Economic Affairs, Agriculture, and Innovation in March 2011.

This recommendation has been met.

Recommendation 4: The State should develop criteria defining unacceptable radiological consequences as a result of a sabotage event.

Response: The IPPAS team noted that this recommendation has been implemented through the new MR.

This recommendation has been met.

Suggestions

Suggestion 1: The State could conduct a periodic review of the trustworthiness of those personnel requiring security clearance.

Response: The Security and Safeguards Coordinator recognized the need for further checks on trustworthiness and was able to brief the IPPAS team that during the visit, further agreement had been reached during the mission with the State authorities responsible for screening, which would allow, *inter alia*, for the periodic review of the trustworthiness of those personnel requiring security clearance. The IPPAS team welcomed this development.

This suggestion has been met.

B. Review of Implementation of New Recommendations (INFCIRC/225/Rev.5 and CPPNMA)

The IPPAS mission was asked to assess whether the new and revised measures for the protection of nuclear material and nuclear facilities in the Netherlands were sufficient to meet the requirements of *INFCIRC/225/Rev.5*, which was published in February 2011. *INFCIRC/225/Rev.5* had been written to ensure consistency with the 2005 *CPPNMA* and it introduces a number of topics which had not been addressed in earlier editions of the document. These topics are:

- risk management: States are expected to manage the risks of theft and sabotage and to keep them at acceptable levels.
- location and recovery of missing nuclear material: *INFCIRC/225/Rev.5* recommends the timely detection of missing nuclear material; a rapid check of a State's nuclear material inventory using nuclear material accountancy and control (NMAC); a system to be in place to notify the appropriate authorities of a loss or theft of nuclear material; off-site pursuit, if necessary; and the securing or return of recovered nuclear material.
- mitigating/minimizing the risk of sabotage: *INFCIRC/225/Rev.5* recommends that security contingency plans and safety emergency plans should be developed to prevent further damage at a site; to secure the nuclear facility; and to protect emergency equipment and personnel. Off-site response forces should also be familiar with the site and with likely sabotage targets, and have sufficient knowledge of radiation protection to operate effectively.
- inclusion of the *Fundamental Principles* and, in particular, an increased emphasis on the application of the graded approach, whereby the level of protection is based upon the assessed threat and the likely consequences.
- computer security: protection should be provided to computer-based systems used for physical protection, nuclear safety, and nuclear material accountancy in a way which is consistent with the threat.
- stand-off attack: barriers should be installed to protect against a stand-off attack from land and water vehicles.
- security culture: acknowledges that a credible threat exists and that the individual plays an important role in preserving nuclear security. Security policy and guidelines should reflect this, and regular training in security should occur to maintain awareness and skills.
- physical protection regime: comprises a State's legislative and regulatory framework; the institutions and organizations within the State that are responsible for ensuring the implementation of the legislative and regulatory framework; and the physical protection systems for nuclear facilities and nuclear transport.
- nuclear material accountancy and control (NMAC) systems: should be integrated with physical protection systems to protect against 'outsider' and 'insider' threats.
- aggregation of nuclear material: the inclusion of all nuclear material inventories within a single facility to enhance the physical protection of all categories of nuclear material held in that facility.
- sustainability programme: encompasses topics such as development of procedures, management of human resources, management of equipment, performance testing, configuration management, resource allocation, and operational cost analysis.

INFCIRC/225/Rev.5 also provided enhanced guidance on:

- the use of a DBT and a State's current evaluation of the threat.
- performance testing: *INFCIRC/225/Rev.5* suggests that regular performance testing of the PPS, including force-on-force exercises, for nuclear facilities with Category I and Category II nuclear material should occur.
- the differentiation between security and safety contingency plans.
- the application of the self-protecting principle.

The new *INFCIRC/225/Rev.5* has been written with a view to incorporating the 2005 *CPPNMA*. It now includes the 12 *Fundamental Principles* and the four *Objectives* of a State's physical protection regime. In addition to the new topics, the team also considered the *Fundamental Principles and Objectives* as part of their review.

The IPPAS team was briefed by the Nuclear Security Policy Coordinator at the Ministry of Economic Affairs, Agriculture and Innovation who reaffirmed the commitment of the Netherlands to implementing the *CPPNMA* (ratified by the Netherlands on 17 April 2011) and adopting the recommendations outlined in *INFCIRC/225/Rev.5*. The Nuclear Security Policy Coordinator acknowledged that the new MR, approved on 7 December 2010, pre-dates *INFCIRC/225/Rev.5* (which was published in February 2011) but he confirmed that these new regulations would be amended appropriately in 2012. The IPPAS team welcomed this commitment.

The programme of visits and the many discussions with the operators, Government officials, off-site responders and NBS throughout the IPPAS mission has allowed the IPPAS team to make an initial assessment of the progress already made towards meeting the requirements of the *CPPNMA* and the *INFCIRC/225/Rev.5* recommendations. From the point of view of the Dutch Legislative and Regulatory Framework, the IPPAS team notes:

- Risk management: There was evidence that this principle was understood by operators and the regulator but was being applied at some sites more effectively than at others.
- Location and recovery of lost or stolen nuclear material: again, there was a clear acceptance of the importance of locating and recovering lost or stolen nuclear material. While the IPPAS team was not briefed on specific plans for the location and recovery of lost or stolen nuclear material, the IBO and EBO contingency planning arrangements provide a basis from which such plans could be developed; this opportunity should be considered.

Basis: *INFCIRC/225/Rev.5* (4.50) — The State should ensure that its physical protection regime includes rapid response and comprehensive measures to locate and recover missing or stolen nuclear material. These location and recovery measures should include on-site and off-site operations.

New Recommendation 1: The IBO and EBO contingency planning arrangements should be considered as the basis upon which plans could be developed for the recovery of lost or stolen nuclear material.

- Mitigate or minimize the risk of sabotage: similarly, the IBO and EBO planning system seems to provide a platform for developing measures to comply with these recommendations and the IPPAS team suggests that this should be considered.

Basis: *INFCIRC/225/Rev.5* (5.13) — The physical protection system against sabotage should be designed as an element of an integrated system to prevent the potential consequences of sabotage by taking into account the robustness of the engineered safety and operational features, and the fire protection, radiation protection and emergency preparedness measures.

New Recommendation 2: The IBO and EBO contingency planning arrangements could provide a platform for the development of measures designed to mitigate or minimize the risk of sabotage.

- Graded approach: the IPPAS team noted that the PPS already reflects the graded approach *Fundamental Principle*.

- Computer security: See Section C below.
- Stand-off attacks: the IPPAS team saw evidence of this recommendation being applied at sites, but took the view that more could be done both in terms of the location of barriers and the robustness of the actual obstacles deployed. The IPPAS team suggests an expert review of the possible options informed by the latest thinking on barrier technology and performance.

New Suggestion 4: An expert review of the options to create stand-off distance (as defined by the DBT) could be conducted at State level, with the aim of assessing how to place barriers to best effect and drawing upon the latest thinking on barrier technology and performance, and the expertise made available as appropriate to Sites.

- Security culture: the IPPAS team acknowledges the clear commitment to security encountered at all levels throughout the visit and the initiatives already taken. The team also acknowledges the view expressed by both the operators and the regulator that maintaining the appropriate security culture is a continuous process and that continuation training should be organized appropriately.
- Physical protection regime: the IPPAS team noted that all components of a physical protection regime were already present in the Netherlands, though at different stages of development. The State should consolidate and continue to improve existing practice.
- Nuclear material accountancy and control (NMAC): the IPPAS team were briefed on the formal procedures in place both through internal State arrangements and Euratom to account for and control nuclear material. While these arrangements were clearly robust, there did appear to be certain inventories where it might be difficult to give precise details in a timely manner. The IPPAS team suggests a review of the NMAC methodology for these inventories so that the Netherlands can comply with both the letter and the spirit of the revised recommendations.

Basis: *INFCIRC/225/Rev.5* (3.26) — The operator should ensure control of, and be able to account for, all nuclear material at a nuclear facility at all times. The operator should report any confirmed accounting discrepancy in a timely manner as stipulated by the competent authority.

New Recommendation 3: The NMAC methodology should be reviewed to enable the prompt and accurate description of inventories to complement physical protection measures to defeat the threat from outsiders and insiders.

- Aggregation of nuclear material: the IPPAS team noted the wish to initiate moves to consolidate holdings of nuclear material to negate the need to meet protection requirements at the LFR, and were briefed on procedural difficulties which were causing delays, particularly with regard to the removal of the HEU from the LFR at Petten.

New Suggestion 5: The State might consider actions to facilitate the prompt removal of highly-enriched nuclear material from the LFR at Petten to COVRA.

Fundamental Principle D, which is now included in *INFCIRC/225/Rev.5*, recommends that States implement measures to ensure effective independence of the State's competent authority from any other body in charge of the promotion or utilization of nuclear energy. As defined by the IAEA General Conference in September 2001, effective independence means that organizational units which are responsible for licensing and supervisory activities are protected by regulatory or organizational

means against any undue influence by other units or bodies on the execution of their tasks. The recent reorganization within the Government has resulted in the separation of nuclear policy from nuclear security inspections. The policy and inspection branches have been split in the recent organizational change. At the current time, both the nuclear policy section and the nuclear inspection branch report directly to the Minister responsible for nuclear energy although the inspection branch is in a different ministry organizationally.

Basis: *INFCIRC/225/Rev.5* (3.18) — The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure an effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy.

New Recommendation 4: The State should review the arrangements in place to ensure effective independence of the competent authority within the Ministry of EL&I to ensure the arrangements meet the intent of *Fundamental Principle D*.

C. Computer Security Provisions at State Level

INFCIRC/225/Rev.5 recommends that computer-based systems used to support important plant operations such as physical protection, nuclear safety, and material accountancy should be protected against compromise.

Computer security was a particular focus of this IPPAS mission, at the request of the Netherlands. The suggestions in this section are made on the basis of NSS No.17, *Computer Security at Nuclear Facilities* (published December 2011), and other industry best practice.

1. Legal and Regulatory Framework for Computer Security

Basis: *NSS No.17* suggests that States carefully consider whether their legislation adequately covers malicious or unintentional acts that may precipitate breaches of nuclear security and that are perpetrated with the aid of computers. This does not necessarily need to be contained in nuclear-related acts and laws. For example, laws that more generally address computer offences or terrorism may already contain sufficient provisions.

New Suggestion 6: The State could consider performing a legal review to verify whether the legal framework contains sufficient provisions to address any future computer-based attacks on a nuclear facility.

Currently, the MR contains several provisions related to information security/confidentiality of sensitive information, but does not contain provisions related specifically to computer security. This makes it difficult for sites to identify and develop necessary and sufficient computer security measures. Furthermore, it could potentially lead to difficulties or inconsistencies across sites when conducting inspections in this area, since there is no common framework for inspectors to refer to.

Basis: *NSS No.17* suggests that States, at a minimum, provide a high level statement of computer security regulatory requirements, and that they consider providing more detailed requirements such as designation of a Computer Security Officer and establishment of a computer security policy and plan (including asset identification, risk management process, training and awareness programme, continuity of operations plan, audit and review process). It is important to note that computer security

does not need to be treated separately from physical protection; these requirements could be addressed either in the site security plan (BIP) or in a separate computer security plan.

New Suggestion 7: The State could consider revising the regulatory framework to include regulatory requirements related to computer security, and ensure that adequately trained personnel are available to provide effective nuclear information security and computer security oversight.

2. Design Basis Threat (DBT)

The IPPAS team understands that the current DBT provided by the State contains little or no detail on cyber-threats; this is planned to be expanded in the next revision of the DBT. One site (Borssele) has developed its own detailed site-level cyber-DBT, which allows computer security measures to be developed in a systematic manner in order to provide protection against a defined threat.

Basis: *NSS No.17* suggests that the relevant State authority should periodically issue a threat evaluation including threats to the security of computer systems. This can be done through the DBT mechanism or any other appropriate threat assessment mechanism.

New Suggestion 8: The State could consider providing cyber-threat information to sites, in the DBT or a similar threat assessment mechanism, to define the cyber-threat(s) that each site must provide protection against.

3. Coordination

Within the Netherlands, ISAC-Nuclear has been established by the operators, for the information and computer security personnel from all nuclear sites to meet periodically and exchange information on challenges, lessons learned, trends, and best practices. This enables all sites to benefit from the experience at each site.

Good Practice [New] 2: Regular meetings of information and computer security personnel across the sites allows for good sharing and exchange of information, observed trends, lessons learned, and best practices.