Lecture 2. FROM PHYSICAL PROTECTION TO NUCLEAR SECURITY

Course “New Challenges to the Nonproliferation Regime”

Dr. Alexey Ubeev

Dual Master’s Degree Program in Nonproliferation Studies
Moscow, Fall - Winter 2016
Definitions, objectives and fundamental principles of physical protection (PP) of nuclear and other radioactive materials and associated facilities

Basic PP system functions, methodology for design and evaluation of effectiveness of PPS (in brief)

Categorization of NM for PP purposes and interface with nuclear materials accountancy and control (NMAC)

Comprehensive approach to Nuclear Security and need for coordination of PPS, NMAC and computer security activities
✓ Physical protection - measures for the protection of nuclear or other radioactive material or associated facilities designed to prevent unauthorized removal, theft or sabotage;

✓ Physical Protection Measures - the personnel, procedures and equipment that constitute a physical protection system (NSS 13);

✓ Physical Protection System (PPS) - an integrated set of physical protection measures intended to prevent completion of a malicious act (NSS 13);

✓ Unacceptable Radiological Consequences (URC) - a level of radiological consequences, established by a State, above which the implementation of physical protection measures is warranted (NSS 13)
✓ **Defence in Depth** - combination of multiple layers of systems and measures that have to be overcome or circumvented before the PP is compromised;

✓ **Threat** - a person or group 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 sources information – that describes the motivations, intentions, and capabilities of these threats;

✓ **Design Basis Threat (DBT)** - attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal or sabotage, against which the physical protection system is designed and evaluated

IAEA NSS №13
**Nuclear material accountancy and control (NMAC)** - an integrated set of measures designed to provide information on, control of, and assurance of the presence of nuclear and other radioactive material. It includes those systems necessary to establish and track nuclear and other radioactive material inventories, control access to and detect loss or diversion of nuclear and other radioactive material, and ensure the integrity of those systems and measures.

**Information security** – the preservation of the confidentiality, integrity and availability of information. (NSS#17)

**Computer security** – a particular aspect of information security that is concerned with computer based systems, networks, and digital systems (NSS #17)

(The terms ‘IT security’ and ‘cyber security’ are considered to be synonyms but not be used in IAEA Nuclear security series publications)
Nuclear Security* - the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts** involving nuclear materials, other radioactive substances, or their associated facilities (IAEA AdSec Group definition)

*Footnote INFCIRC 225/Rev.5 indicates “Historically, the term “physical protection” has been used to describe what is now known as the nuclear security”

**Examples of malicious acts are also: unauthorised removal, diversion, sabotage

Nuclear security is more comprehensive than physical protection. Nuclear security definition specific to nuclear and other radioactive materials and facilities and is inclusive of physical protection, personnel, information and computer (cyber) security as well as nuclear material accountancy and control (NMAC).

Nuclear security needs full and universally accepted definition
The Twelve Fundamental PP Principles

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A:</td>
<td>Responsibility of the State</td>
</tr>
<tr>
<td>B:</td>
<td>Responsibilities During International Transport</td>
</tr>
<tr>
<td>C:</td>
<td>Legislative and Regulatory Framework</td>
</tr>
<tr>
<td>D:</td>
<td>Competent Authority</td>
</tr>
<tr>
<td>E:</td>
<td>Responsibility of the License Holders</td>
</tr>
<tr>
<td>F:</td>
<td>Security Culture</td>
</tr>
<tr>
<td>G:</td>
<td>Threat</td>
</tr>
<tr>
<td>H:</td>
<td>Graded Approach</td>
</tr>
<tr>
<td>I:</td>
<td>Defence in Depth</td>
</tr>
<tr>
<td>J:</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>K:</td>
<td>Contingency Plans</td>
</tr>
<tr>
<td>L:</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

2005 Amendment to CPPNM
The objectives of the State’s physical protection regime, which is an essential component of the State’s nuclear security regime, should be:

- To protect against unauthorized removal. Protecting against theft and other unlawful taking of nuclear material.

- To locate and recover missing nuclear material. Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material.

- To protect against sabotage. Protecting nuclear material and nuclear facilities against sabotage.

- To mitigate or minimize effects of sabotage. Mitigating or minimizing the radiological consequences of sabotage.
The State’s physical protection regime should seek to achieve these objectives through:

• Prevention of a malicious act by means of deterrence and by protection of sensitive information;

• Management of an attempted malicious act or a malicious act by an integrated system of detection, delay, and response;

• Mitigation of the consequences of a malicious act.
Physical Protection Regime

- Legislative and Regulatory Framework
- Institutions and Organizations
- Physical Protection Systems
Physical Protection Regime Institutions

- State
- Competent Authority
- Licence Holders
  - Operator of nuclear facilities
  - Shipper and receiver for transport of nuclear materials

Nuclear Security Culture crosses all three levels
State Responsibilities for PP Regime

State

- Legal and Regulatory Framework
- Assignment of Responsibilities
- Physical Protection Requirements
- International Transport
- International Cooperation
Basic PP system Functions

**Detection:** process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm.

**Delay:** the element of a physical protection system designed to increase adversary penetration time for entry into and/or exit from the nuclear facility or transport.

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

Sensor Activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed

“An alarm without assessment is not detection.”

Delay

Provide obstacles to increase adversary task time after detection

Response

Communicate to Response Force → Deploy Response Force → Interrupt and Neutralize Adversary Attempt
**Role of Delay**

System detection and response time must be less than adversary task time after first alarm.

- To increase system success probability
  - Detect intrusion earlier
  - Reduce assessment time
  - Reduce response time
  - Increase adversary task time

(IAEA Training Material)
Forcible Entry Example

<table>
<thead>
<tr>
<th>Task</th>
<th>Mean Time (seconds)</th>
<th>Cumulative Time (seconds)</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12</td>
<td>24</td>
<td>Climb over fence</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>72</td>
<td>Run 76 m</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
<td>96</td>
<td>Force door</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
<td>108</td>
<td>Walk 45 m</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>114</td>
<td>Cut lock</td>
</tr>
<tr>
<td>6</td>
<td>06</td>
<td>126</td>
<td>Walk to container</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>180</td>
<td>Open container and gather material</td>
</tr>
<tr>
<td>8</td>
<td>54</td>
<td>180</td>
<td>Escape</td>
</tr>
</tbody>
</table>

Total time for adversary. Approx. 3 minutes

(IAEA Training Material)
Design and Evaluation
Process Outline (DEPO) for PPS

Define PPS requirements

Process of design & evaluation

Facility characterization

Target Identification

Threat definition

Design PPS

Physical Protection System

Detection

Intrusion detection

Alarm Assessment

Access control

Alarm Communication & display

Evaluate PPS

AsD

Single Path analysis

Neutralization analysis

Scenario analysis

Insider analysis

Final PPS Design

Rev Design PPS
Categorization is the basis for a graded approach for protection against unauthorized removal of nuclear material (NM) that could be used in a nuclear explosive device.

IAEA categorizes the different types of NM in terms of element, isotope, quantity and irradiation.

Nuclear operator should assess and manage the physical protection interface with safety and NM accountancy and control activities.

Systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise consistent with the threat assessment or design basis threat.
# IAEA Categorization of NM for PP

<table>
<thead>
<tr>
<th>Material</th>
<th>Category I</th>
<th>Category II</th>
<th>Category III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plutonium</td>
<td>2 kg or more</td>
<td>2… 0.5 kg</td>
<td>500… 15 g</td>
</tr>
<tr>
<td>HEU-235</td>
<td>5 kg or more</td>
<td>5… 1 kg</td>
<td>1000… 15 g</td>
</tr>
<tr>
<td>LEU 10-20%</td>
<td>-</td>
<td>10 kg or more</td>
<td>10… 1 kg</td>
</tr>
<tr>
<td>LEU less 10%</td>
<td>-</td>
<td>-</td>
<td>10 kg or more</td>
</tr>
<tr>
<td>Irradiated fuel</td>
<td>-</td>
<td>Depleted or natural or LEU</td>
<td>-</td>
</tr>
</tbody>
</table>

Categories for unirradiated Pu and U (see more for LEU, U-233 and irradiated NM in IAEA NSS-13)
Limited Access Area (new concept): limited and controlled access

Clarification on site areas (NSS 13)

- Physical protection personnel are not expected to know precisely the nature of operations to be performed on nuclear material or with facility equipment in controlled areas (e.g. in NM process area)

- It is not duty of PP staff to determine the nature and quantities of nuclear material

- PP staff could hardly detect some preparations of NM for theft
  - Unauthorized operations with NM by insiders
  - Manipulations with measurement equipment or falsification of measurement results
  - Unauthorized relocation of NM items or their preparation for unauthorized shipment, etc.
Example. Difficulties in detection of possible unauthorized NM removal by insider. **NMAC system.**

- NM accountancy and control at NM locations
  - NMAC at many facilities is focused on accurate accounting during only periodic inventories
  - Difficulties in timely detection of NM theft
  - Effectiveness of NMAC for nuclear security is very questionable if information about lost NM would be available only after annual inventory when response measures and recovery of stolen NM might not be effective
Computer and Information Security

Computer based systems used for

- **physical protection**, 
- **nuclear safety**, 
- **nuclear material accountancy and control**

“should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat.” (NSS#13)

Most of these system exist as a complex network of embedded systems and computers which just like a desktop computer or a industrial control system, **are subject to compromise and attack.**
The IAEA NS Computer and Information Security programme is focused on preventing computer acts that could directly or indirectly lead to:

a. **unauthorized removal** of nuclear/other radioactive material

b. **sabotage** against nuclear material or nuclear facilities

c. **theft** of nuclear sensitive information
Information and Computer Security are not isolated domains, but are interlinked with the other aspects of security.
Types of Network Attacks

**Denial of service (DOS)/Loss of Function**
Block operator’s ability to observe and/or respond to changing system conditions, slow the system to a crawl

**Unobserved System Monitoring & Data Collection**
Unauthorized file access and data recording
Message (information) interception

**Interception (Man in the Middle)**
Interception and modification of data stream between nodes

**Operator Spoofing leading to Incorrect Action**
Causing operator to take incorrect action.
**Direct manipulation of computer/control system**

Ref: Tutănescu, Ion, Ass. Prof., Ph.D., Prof. Emil Sofron, Ph.D., Anatomy and Types of Attacks against Computer Networks, Department of Electronics and Computers, University of Pitești, ROMANIA.
Humans are typically the weakest link

10 risky practices which in which employees routinely engage:  [ref: Ponemon, 2012]
1. Connecting computers to the Internet through an insecure wireless network.
2. Not deleting information on their computer when no longer necessary.
3. Sharing passwords with others.
4. Reusing the same password and username on different websites.
5. Using generic USB drives not encrypted or safeguarded by other means.
6. Leaving computers unattended when outside the workplace.
7. Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
8. Working on a laptop when traveling and not using a privacy screen.
9. Carrying unnecessary sensitive information on a laptop when traveling.
10. Using personally owned mobile devices that connect to their organization's network.

Nuclear Security at Facility

- Main contributors to nuclear security depending on threat (considering both insiders and ‘outsiders’)
  - NM theft: PP and NMAC, computer security
  - Sabotage: PP, nuclear and radiation safety, operation features, computer security

- Each facility system has technical limitations in prevention of adversary scenarios

- None of facility systems alone is able to prevent all feasible adversary scenarios, if threat was not eliminated

- Coordination of all contributing facility systems is required for effective nuclear security
Nuclear Security coordination at the facility (PPS + NMAC + Computer security +...)

NMAC, PP system and computer security measures should be designed to work together for detection and prevention of all types of nuclear material theft or sabotage and proper response to

There is a principal difference between the material control measures and corresponding physical protection measures

- They are applicable to different locations in the facility:
  - NMAC measures are for the immediate vicinity of nuclear material, and
  - Physical protection measures are for other locations, such as protected areas or material access areas
- Their control measures are performed by different facility personnel
Nuclear Security coordination at facility (PPS + NMAC + Computer security +...), cont’d

What information does the physical protection system need from NMAC?
- Locations and characteristics of nuclear material
- Results of emergency inventory, if one is taken
- Authorized shipment information
- Material Control measures that have been implemented
- Authorized locations for nuclear material

What information does the NMAC System need from physical protection?
- Area access information
- Access authorizations
- Information about alarm conditions or irregularities

What information does the computer security need from PPS and NMAC? - All above-mentioned at “need to know” basis
Physical protection is the essential part, but not cover all aspects of nuclear security. Nuclear security needs full and universally accepted definition.

Twelve fundamental principles of PP are the solid base for establishment of effective State’s PP regime.

Detection, delay and response interface are the main functions of effective PP systems for nuclear facility.

NMAC for Nuclear Security has some differences from MC&A for safeguards purposes.

PPS, NMAC and Computer security are the integral parts of Nuclear Security and need close cooperation.
Thank you for your attention!

*Special thanks to the IAEA Nuclear Security Division Staff for kind assistance*

Questions?