

**SPESS F**  
**Document Preparation Profile (DPP)**  
**Version 0 dated 18 March 2016**

## 1. IDENTIFICATION

|                                      |   |
|--------------------------------------|---|
| <b>Document Category</b>             | <b>Implementing Guide</b>   |
| <b>Working ID:</b>                   | <b>NST058</b>   |
| <b>Proposed Title:</b>               | <b>Development, Use and Maintenance of Threat Assessment and Design Basis Threat</b>                |
| <b>Proposed Action:</b>              | <b>Revision of NSS 10, “Development, Use and Maintenance of the Design Basis Threat” (May 2009)</b> |
| <b>Review Committee(s) or Group:</b> | <b><u>NSGC</u>, all SSCs (to be confirmed by Interface Group)</b>                                   |
| <b>Technical Officer(s):</b>         | <b>Sanjay Parulkar</b>  |

## 2. BACKGROUND

The Design Basis Threat (DBT) was introduced in Revision 4 of INFCIRC/225 in 1999, which is developed from an evaluation of a threat assessment carried out by the State for unauthorized removal of nuclear material and of sabotage of nuclear material and nuclear facilities. Threat assessment is an essential element of a State’s nuclear security regime and the IAEA recommends using the DBT as a common basis for physical protection planning by the operator and approval by the competent authority of the physical protection system.

Nuclear Security Series No. 10, “**Development, Use and Maintenance of the Design Basis Threat**” was published by IAEA as an Implementing Guide in May 2009.

The reference documents in NSS 10 are *INFCIRC/225/Rev4 (Corrected)* of 1999, the *Physical Protection Objectives and Fundamental Principles (GOV/2001/41)*, the Convention on the Physical Protection of Nuclear Material (CPPNM). *INFCIRC/225/Rev4 (Corrected)* addresses the need for protection of sensitive information but does not address computer security and cyber threats.

The IAEA has convened several consultancy meetings to discuss the implementation of cyber specific threat assessments in the threat assessment and DBT process. The experts concluded that the methodology described in NSS 10 is useful and applicable in principle for all credible threat assessments and DBT. Cyber specific threats should be elaborated in more detail and integrated in NSS 10.

## 3. JUSTIFICATION FOR THE REVISION OF THE DOCUMENT

NSS 10 was published prior to the publication of the Nuclear Security Series Fundamentals (NSS 20) and the Recommendations-level documents (NSS 13, 14 and 15). As such, a revision is needed to update NSS 10, including for consistency with terminology used in newer publications of the Nuclear Security Series and to reflect new guidance as well. In addition to consistency, further reasons for the revision of the Guide are provided below.

Firstly, paragraph 4.10 of NSS No. 13, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Rev5) states that computer based systems used for physical protection, nuclear safety systems and nuclear material accountancy and control systems should be protected against compromise (e.g. cyber-attack, manipulation and falsification) consistent with the threat assessment or design basis threat. As such, simply noting “cyber skills” in the list of attributes and characteristics in the current NSS 10 is not providing sufficient guidance for States to achieve the consistency with the threat assessment or DBT as required by paragraph 4.10 of NSS 13. This was further confirmed during the TM on *Conducting Cyber Threat Assessments at Nuclear Facilities* held in February 2016 when Member States identified the need for consideration of cyber specific threats when defining DBT.

Secondly, during the *International Workshop on the Lessons Learned from Design Basis Threat and the Use of a Threat-Based Approach for the Regulation of Nuclear Material and Nuclear Facilities* held in July 2014, Member States expressed concern that in the current version of NSS 10, there is an ambiguity with the use of the term ‘threat assessment’ as an alternative approach to the DBT. The revision of NSS 10 will clarify terminology with respect to alternative approaches to the DBT.

The third reason for revising NSS 10 was another outcome of the above-mentioned workshop wherein Member States expressed that NSS 10 does not sufficiently explain how to develop application-specific DBTs such as a facility-specific or transport-specific DBT.

Finally, further guidance is needed to address the possibility of insider threats using or supporting cyber capabilities or cyber skills, given this area has grown significantly since the publication of NSS 10. The previously mentioned CMs, TMs and workshops noted that further guidance for DBT development is needed in this regard.

#### **4. OBJECTIVE**

The objective of reviewing NSS 10 is to provide detailed guidance to States’ Competent Authorities / Regulators on a threat-based approach to establish security requirements, and to design and evaluate physical protection systems, taking into account all credible threats in a well-coordinated way.

The revised publication will provide clear structured guidance on how to go through a logical process from an evaluation of threats through a decision-making process to a threat statement like DBT or an Alternative Threat Statement (ATS) to be used as a basis for evaluation of security requirements.

The revision of NSS 10 will also provide guidance on how to apply the DBT methodology for ATS when a DBT is not required or feasible for example for the evaluation of security requirements for radioactive sources or Category II nuclear material. This guidance will expand on the recommendations of NSS 14 on threat assessment.

The revised NSS 10 will describe on how to use the results of this logical process, DBT or ATS, as basis for evaluation of security requirements for the protection of nuclear and other radioactive material, associated facilities and activities of all categories and how to adjust to the specifics of individual use, storage and transport.

It will reflect the coordinated consideration of attributes and characteristics of all credible threats relevant for physical attacks as well as cyber capabilities and cyber skills for cyber-attacks and

blended attacks (Cyber/physical) guiding to consistent requirements for design and evaluation of nuclear security systems including physical protection measures and computer security measures.

The revision of NSS 10 will provide clearer guidance on how to use the DBT for design and evaluation of physical protection systems when applying the concepts contained in NSS 13 and in the Implementing Guide NST023 on performance evaluation of security systems.

## **5. SCOPE**

It is intended to keep the revision of NSS 10 as an Implementing Guide in the hierarchy of the Nuclear Security Series.

The scope of a revised NSS 10 will be the development, use and maintenance of threat assessment and the DBT as a basis for the design, establishment, and evaluation of physical protection measures for nuclear and other radioactive material, associated facilities and associated activities. It will provide guidance for the application of the DBT methodology in an alternative threat-based approach (ATS) for the security of other radioactive material, associated facilities and associated activities consistent with the guidance provided in NST048 (revision of NSS No. 11 currently out for MS comments). It will provide guidance to Competent Authorities in defining threat-based security requirements for the design of security systems against all credible threats.

The revision of NSS 10 will not address threat assessment for material outside of regulatory control which is covered by NSS 24-G.

## **6. PLACE IN THE OVERALL STRUCTURE OF THE RELEVANT SERIES AND INTERFACES WITH EXISTING AND/OR PLANNED PUBLICATIONS**

It is proposed that the revised NSS 10 document should stay as an implementing guide. The document will reside under and will elaborate on the recommendations and guidance provided in:

- INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2012)
- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011)
- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011)
- NST023 – Implementing Guide for NSS 13
- NST048 –Security of Radioactive Material in Use and Storage and of Associated Facilities (revision of NSS 11)

Regarding interfaces, it is foreseen that this document will not have interface with nuclear radiation, waste, transport and safety. As such, it will be developed in consultation with colleagues from the relevant divisions as appropriate, as well as provided to all SSCs for clearance. [Subject to Interface Group decision]

## 7. OVERVIEW

As a starting point, the contents of the current NSS 10 will be revised with additional content to be added regarding cyber threats and considerations.

### PROPOSED TABLE OF CONTENTS

1. INTRODUCTION
  - 1.1. Background
  - 1.2. Objective
  - 1.3. Scope
  - 1.4. Structure
2. THREAT ASSESSMENT OR DBT IN A RISK INFORMED APPROACH
  - 2.1. Assets and Consequences
  - 2.2. Threats and Relative Attractiveness of assets
3. THREAT ASSESSMENT OR DBT A REGULATORY TOOL
  - 3.1. Assignment of Responsibilities for Security
  - 3.2. Definition of Security Requirements
  - 3.3. DBT and Alternatives to DBT
  - 3.4. DBT as a Threat Statement
4. DESCRIPTION OF A *DESIGN BASIS THREAT*
  - 4.1. Attributes and Characteristics of adversaries
  - 4.2. DBT(s) Adjusted to Specific Needs
5. CONSIDERATIONS OF PHYSICAL THREATS AND CYBER CAPABILITIES IN *DESIGN BASIS THREAT*
  - 5.1. Need for coordinated Design Basis Threat / ATS
  - 5.2. Attributes and Characteristics of Physical Threats
    - 5.2.1. Threats from Outside Including Stand-Off Threats
    - 5.2.2. Insider Threat
  - 5.3. Attributes and Characteristics of Cyber specific Threats
    - 5.3.1. Cyber specific Threats from Outside
    - 5.3.2. Insider Cyber specific Threats
  - 5.4. Integration / coordination of Attributes and Characteristics
6. ROLES AND RESPONSIBILITIES FOR DEVELOPMENT, USE AND MAINTENANCE OF A DBT
  - 6.1. State
  - 6.2. Cyber and Information Security Authorities
  - 6.3. Intelligence Organizations
  - 6.4. Operators
  - 6.5. Other Organizations
7. PERFORMING A THREAT ASSESSMENT
  - 7.1. Description of a Threat Assessment
  - 7.2. Input
  - 7.3. Process of Analysis
  - 7.4. Output
  - 7.5. Cyber Specific Threat Considerations

- 7.5.1. Threat profiles and attributes
- 7.5.2. Threat multipliers
- 7.5.3. Attack Vectors
- 7.5.4. Logical mapping of attacks (Domain based attacks)
- 7.5.5. Attack frequency
- 8. DEVELOPING AN INTEGRATED / COORDINATED APPROACHES
  - 8.1. Inputs to Design Basis Threat / ATS
  - 8.2. Process of Screening, Translating, Decision Making
  - 8.3. Outputs
- 9. USING THREAT BASED APPROACH FOR DESIGN AND EVALUATION OF SECURITY SYSTEMS AND MEASURES
  - 9.1. Information security Considerations
  - 9.2. Defining Performance Requirements for Security Measures
  - 9.3. Defining Requirements for Implementing Security Measures in a Prescriptive Approach
  - 9.4. Developing attack scenarios for Design and Evaluation of Security Systems requirements
    - 9.4.1. Physical Attack Scenarios
    - 9.4.2. Cyber Attack Scenarios
    - 9.4.3. Blended Attacks by Physical and Cyber attacks
- 10. MAINTAINING THE DESIGN BASIS THREAT / ATS
  - 10.1. Input
  - 10.2. Process
  - 10.3. Output
  - 10.4. Process for of Cyber Specific Threat Changes for immediate Consideration

## 8. PRODUCTION SCHEDULE:

|  | B*                |
|--|-------------------|
| STEP 1: Preparing a DPP  | March 2016        |
| STEP 2: Approval of DPP by the Coordination Committee  | April 2016        |
| STEP 3: Approval of DPP by the relevant review Committees  | NSGC in June 2016 |
| STEP 4: Approval of DPP by the CSS   |                   |
| STEP 5: Preparing the draft;   |                   |
| STEP 5b: TM is expected to be organized for the preparation of the draft   | Q1 2017           |
| STEP 5c: Consultancy Meeting to incorporate comments from MSs during technical meeting (1-2 depending on extent of comments) | Q2 2017           |
| STEP 6: Approval of draft by the Coordination Committee  | Q3 2017           |
| STEP 7: Approval by the relevant review Committees for submission to Member States for comments                              | Q4 2017           |
| STEP 8: Soliciting comments by Member States   | Q1-2 2018         |
| STEP 9: Addressing comments by Member States   | Q3 2018           |
| STEP 10: Approval of the revised draft by the Coordination Committee<br>Review in NS-SSCS                                    | Q3 2018           |
| STEP 11: Approval by the relevant review Committees  | Q4 2018           |

|  |         |
|--|---------|
| STEP 12: Endorsement by the CSS  |         |
| STEP 13: Establishment by the Publications Committee and/or Board of Governors (for SF and SR only)) | Q4 2018 |
| STEP 14: Target publication date   | Q4 2018 |

Although this is a revision of an existing Implementing Guide, it is proposed to hold a Technical Meeting as part of the development process. A TM is proposed in view of the extension of the scope of the Implementing Guide, particularly in relation to cyber Specific threats and alternative approaches to DBT.

## **9. RESOURCES**

It is foreseen to have 4-5 consultancy meetings to develop the initial draft of the document followed by one Technical Meeting for the review of the initial draft. One or two additional consultancy meetings will then be required to incorporate comments from Member states during Technical Meeting. The outcome of these consultancy meetings will then be a revised draft, which will be submitted to the NSGC for approval and other SSCs for clearance to be distributed to MSs for comments (120 days review). The draft will then be submitted to the NSGC and relevant SSCs for the final approval for publication.