SPESS F
Document Preparation Profile (DPP)
Draft Version 10, 26 August 2020

1. IDENTIFICATION

Document Category: **Nuclear Security Series – Technical Guidance**

Working ID: **NST 065**

Proposed Title: **The Establishment and Implementation of a Trustworthiness Programme in Nuclear Security**

Proposed Action: **New document**

Review Committee(s) or Group: **NSGC**

Technical Officer(s): **Robert Larsen**

2. BACKGROUND

Trustworthiness programmes are a vital component of effectively mitigating threats posed by insiders within a State's nuclear security regime. Such programmes aim to reduce the risk of the threat posed by insiders by fostering integrity, honesty and reliability and by limiting access to locations that could be the target of a malicious act involving nuclear or other radioactive material and to security-sensitive systems and information. An individual's authorized access is limited when serious doubts are established regarding their integrity, honesty and reliability.

In nuclear security, trustworthiness has essentially its dictionary meaning. However, the specific context implies that the concern is whether a person might, by act or omission, commit, facilitate or otherwise assist in the commission of a *malicious act*. The concern relates to acts or omissions that the person might commit intentionally. However, 'intentionally' may include acts or omissions committed with or without a significant degree of understanding of an ultimate purpose and potential consequences. This could include:

- Knowing of the participation in a malicious act by or on behalf of a directly motivated adversary;
- Participation in or facilitation of, with or without full understanding, a malicious act in return for a personal benefit (e.g. payment);
- Participation in or facilitation of, with or without full understanding, a malicious act under duress (e.g. blackmail, coercion, extortion or other threat).

The need to carry out trustworthiness checks or assessments is invoked in all three NSS recommendation-level guidance documents: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev. 5) (NSS No 13), Nuclear Security Recommendations on Radioactive Material and Associated Facilities (NSS No 14) and Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control (NSS No 15). Moreover, NSS No 13 recommends the establishment of a State trustworthiness policy and mechanism to satisfy, in part, Fundamental Principles C and L contained in the amended

Convention on the Physical Protection of Nuclear Material (ACPPNM). Furthermore, the establishment of a trustworthiness programme would support a State's obligations under the United Nations Security Council Resolution 1540.

Trustworthiness also appears as a concept in *Preventive and Protective Measures against Insider Threats* (NSS No 8-G Rev. 1), an NSS Implementing Guide, which recommends that trustworthiness assessments should be used to provide an initial assessment (during the hiring process) and ongoing assessments (periodically throughout the employment period). Other NSS guidance advising the establishment of personnel trustworthiness programmes includes *Nuclear Security Culture* (NSS No 7), *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities* (NSS No 25-G), *Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control* (NSS No 21), and *Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control* (NSS No 36-G).

However, guidance on how to effectively design and implement trustworthiness programmes is not provided in existing NSS documents. While NSS No 8-G (Rev. 1) recognises that trustworthiness assessments are encouraged as a preventive measure for insider threat mitigation, it does not provide details on the criteria for establishing trustworthiness or how a trustworthiness programme should be managed. Likewise, NSS No 7 suggests that States "establish requirements for the determination of personnel trustworthiness." NSS No 25-G states that "determination of trustworthiness" should constitute part of the access authorization process for handling of nuclear material but does not detail ways in which this could be done.

3. JUSTIFICATION FOR THE PRODUCTION OF THE DOCUMENT

As described above, trustworthiness checks and assessments are recommended in multiple NSS guidance documents and are a necessary instrument for satisfying the Fundamental Principles set forth in the ACPPNM. NSS No 8, which addresses the insider threat, was recently revised (published early 2020), and it was decided at that time that the level of detail needed to provide sufficient information on trustworthiness was not appropriate for an Implementing Guide. There is no other publication that currently exists in the NSS where it would be appropriate to include this level of detailed information on this topic.

The NSGC recognized the need for providing detailed guidance on trustworthiness programmes and requested that an outline for a guidance publication be developed by the Secretariat and provided to the 15th NSGC meeting in July 2019. Following discussion at this meeting, a revised outline was presented and discussed at the 16th NSGC meeting in November 2019, where a DPP for a technical guidance publication was requested in advance of the next NSGC meeting.

4. OBJECTIVE

The objective of the proposed publication is to provide guidance on the elements of an effective trustworthiness programme to support Member States in designing and implementing trustworthiness programmes for mitigating threats posed by insiders.

The audience for the proposed publication includes competent authorities, operators and other stakeholder organizations with responsibilities for the security of nuclear material in use, storage and transport and nuclear facilities, as well as for other radioactive material in use storage and transport and associated facilities and associated activities. As trustworthiness guidance contained in this document will also aid in the prevention, detection, and response to nuclear security events involving nuclear and other radioactive material out of regulatory control, law enforcement, border security, and technical expert support are also seen as a potential audience.

5. SCOPE

The proposed publication will describe the measures of an effective trustworthiness programme and considerations for how to apply trustworthiness assessments using the graded approach for threats posed by insiders within competent authorities and other stakeholder organizations.

States may have different ways of implementing these measures consistent with their national legislative and regulatory frameworks; therefore, the proposed publication will not specify how a Member State should implement the measures or gather information to support trustworthiness assessments but rather will describe the main components of a trustworthiness programme.

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

As the concept of trustworthiness is applied across the scope of IAEA guidance for the security of nuclear material, other radioactive material, and material out of regulatory control (MORC), the proposed publication will be a cross-cutting Technical Guidance (TG) document within the Nuclear Security Series (NSS). As Technical Guidance, it will also directly support implementation of insider threat mitigation activities covered by NSS No 8-G, Rev. 1 and NSS No 36-G.

The proposed publication will also interface with other NSS publications that explicitly call for trustworthiness assessments, including:

- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G, Rev.1, IAEA, Vienna (2020).
- 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).
- EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

- INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

- INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

- INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

- INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 36-G, IAEA, Vienna (2019).

7. OVERVIEW

The suggested outline of the proposed Technical Guidance is as follows:

1. Introduction
- 1.1. Background
- 1.2. Objective
- 1.3. Scope
- 1.4. Structure

2. Overview of Trustworthiness Programmes
- 2.1. Benefits of a trustworthiness programme as preventive and protective measures
- 2.2. Methodologies for determining trustworthiness
- 2.3. Interfaces with nuclear security culture programmes
- 2.4. Interfaces with other IAEA Guidance and international agreements

3. State Nuclear Security Regime - Legislative and Regulatory Framework
- 3.1. Legislative considerations
- 3.2. Regulatory considerations
- 3.3. Roles in Trustworthiness Programme Implementation
  - 3.3.1. Regulatory Bodies
  - 3.3.2. Other Competent Authorities
  - 3.3.3. Operators
  - 3.3.4. Other stakeholders

4. Implementing Trustworthiness Programmes in the Nuclear Security Regime Using a Graded Approach
- 4.1. Establishing graded levels of trustworthiness requirements
- 4.2. Process and criteria for determining which individuals are subject to specific levels of trustworthiness determination (depending on the risk and potential consequences of adverse impact)

5. Establishing Guidelines for Making Trustworthiness Determinations/assessments
- 5.1. Determination of graded, consistent trustworthiness criteria for access authorization
- 5.2. Basis for establishing consistent trustworthiness criteria under prescriptive, performance based, or combined approaches

5.2.1. When to conduct verification in accordance with legislation (e.g. identity, employment, education, financial, behavioural, substance abuse, medical and psychological)
5.2.2. When to conduct a reassessment (e.g. continuously, periodicity or change in status like conviction, debt, illness, trauma, extended absence, or presence of other significant life stressors)
5.2.3. Considerations on balancing data privacy and trustworthiness determinations
5.2.4. Motivational or behavioural characteristics of insider adversaries

6. Procedures for Implementation

6.1. Roles and responsibilities
6.1.1. Regulatory bodies
6.1.2. Other competent authorities (including law enforcement)
6.1.3. Operators
6.1.4. Other stakeholders
6.2. Process for trustworthiness determination
6.3. Inputs to access authorization process
6.4. Notification of results
6.5. Transferring authorization
6.6. Periodic and ongoing reassessment

7. Documenting Process, Results of Determinations and Access Authorizations

7.1. Type of documentation (paper and electronic format)
7.2. Record retention (paper and electronic format)
7.3. Tracking access authorizations
7.4. Tracking access suspensions/denials/withdrawals or limitation

8. Administrative Actions

8.1. Granting of access authorization
8.2. Reduction of access authorization of an individual under investigation
8.3. Suspension and termination of access authorization
8.4. Reinstatement of access authorization
8.5. Removal of trustworthiness determination when it is no longer needed
8.6. Responsibilities and liabilities
8.6.1. Personal responsibility for conducting trustworthiness procedures
8.6.2. Responsibility of authorities providing information for trustworthiness procedures
8.6.3. Responsibilities of license holders
8.6.4. Liability for personal information disclosure
8.6.5. Fees, penalties, restrictions and privileges
8.7. Sanctions

9. Protections for Personnel Subject to Trustworthiness Programmes

9.1. Informed consent
9.2. Appeals process
9.3. Workplace support (e.g., employee assistance programmes, whistle-blowing protection)

10. Reporting Requirements

10.1. Behaviours of concern

10.2. Reporting
    10.2.1. Direct observation
    10.2.2. Third-party
10.3. Self-reporting
10.4. When to report
10.5. Chain of command for reporting
10.6. Conducting an inquiry
10.7. Confidentiality and non-reprisal

11. Information Protection

11.1. Requirements for background screeners, access authorization programme personnel
11.2. Data privacy requirements

12. Continuing Effectiveness

12.1. Audits, corrective actions, and follow-ups to corrective actions
12.2. Integrated approach (e.g., security, human resources, training)
12.3. Regulatory oversight of a trustworthiness programme
12.4. Interface with the threat statement and/or design basis threat

13. Addressing Specific Challenges

13.1. Decision-making under risk
    13.1.1. Susceptibility to authority
    13.1.2. Susceptibility to coercion
    13.1.3. Susceptibility to collusion
    13.1.4. Susceptibility to bribery
13.2. Foreign personnel
13.3. Contractors and Temporary workers
13.4. Students and interns
13.5. Supply chain
13.6. National laws pertaining to privacy protection
13.7. National or regional culture
13.8. Different vetting processes/standards used by different organizations
13.9. Visitors

8. PRODUCTION SCHEDULE

Provisional schedule for preparation of the document, outlining realistic expected dates for each step:

STEP 1: Preparing a DPP	March 2020
STEP 2: Approval of DPP by the Coordination Committee	April 2020
STEP 3: Approval of DPP by the relevant review Committees	June 2020
STEP 4: Approval of DPP by the CSS	
STEP 5: Preparing the draft Indicate as to whether a TM is expected to be organized for the preparation of the draft	July 2020- July 2021
STEP 6: Approval of draft by the Coordination Committee	September 2021
STEP 7: Approval by the relevant review Committees for submission to Member States for comments	November 2021
STEP 8: Soliciting comments by Member States	December 2021- February 2022
STEP 9: Addressing comments by Member States	March 2022
STEP 10: Approval of the revised draft by the Coordination Committee Review in NSOC-SGDS (Technical Editorial review)	September 2022
STEP 11: Approval by the relevant review Committees	November 2022
STEP 12: - Submission to the CSS - Submission in parallel and approval by the Publications Committee - MTCD Editing - Endorsement of the edited version by the CSS	
STEP 13: Establishment by the Publications Committee and/or Board of Governors (for SF and SR only))	n/a
STEP 14: Target publication date	2023

*

- *Column A for Safety Fundamentals, Safety Requirements and Safety Guides.*
- *Column B for Nuclear Security Series publications*
- *Column C for TECDOCs, safety reports and other publications*

9. RESOURCES

It is estimated that development of the Technical Guidance will involve approximately 32 weeks of effort by Member States experts. This is based upon assuming 2 one-week expert meetings involving an average of 8 experts and an average of 2 weeks of work per expert between meetings. Secretariat resources involved are estimated at 8 weeks of effort by Agency staff plus support for expert travel and honoraria for experts whose effort is not otherwise funded. A Technical Meeting should be conducted at the beginning of the development of the document to identify as many good practices in this area as possible.