SPESS F
Document Preparation Profile (DPP)
Version 2 dated 17 March 2022

1. IDENTIFICATION

Document Category or batch of publications to be revised in a concomitant manner

Nuclear Security Implementing Guide

Working ID: **NST070**

Proposed Title: **Information Security for Nuclear Security**

Proposed Action: **Revision of a publication**

NSS No. 23-G, Security of Nuclear Information (2015)

Review Committee(s) or Group: **NSGC and all Safety Standards Committees**

Technical Officer(s): **Mr. Mitchell Hewes (NSNS/INMA)**

2. BACKGROUND

Nuclear security seeks to prevent, detect, and respond to malicious acts involving nuclear and other radioactive material and associated facilities and associated activities. Groups or individuals wishing to plan or commit any malicious act involving nuclear material or other radioactive material or associated facilities and associated activities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with the appropriate measures. Sensitive information is information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.

The IAEA has developed a set of nuclear security publications to support Member States in establishing and enhancing information security and computer security for nuclear material and nuclear facilities and other radioactive material and associated facilities and associated activities.

The existing implementing guide on information security, IAEA Nuclear Security Series No. 23-G "*Security of Nuclear Information*" (NSS No. 23-G), was published in 2015. The IAEA has subsequently published IAEA Nuclear Security Series No. 42-G "*Computer Security for Nuclear Security*" (NSS No. 42-G) in 2021 to provide detailed guidance on computer security as a subset of information security, with both Implementing Guides considered cross-cutting for all topics covered by the Nuclear Security Recommendations contained in NSS Nos 13, 14 and 15.

The guidance contained in NSS No. 42-G places an emphasis on maintaining the integrity and availability of information for both computer security and information security. This was primarily to address the following aspects of the relationship between information security and computer security: (i) the ability for computer based systems to aggregate and transmit large quantities of information thereby increasing the sensitivity of a compromise; (ii) the reliance on computer based systems to take automated real physical actions based on data that may be classified as sensitive information; and (iii) the susceptibility of this information to manipulation or falsification, causing an incorrect action to be undertaken by an automated system or human operator.

3. JUSTIFICATION FOR THE PRODUCTION OF THE PUBLICATION

In 2021, the Secretariat reviewed NSS No. 23-G and identified several areas where the current publication of NSS No. 23-G needs updating. These areas include updates to make the publication more cross-cutting with respect to nuclear material and facilities, other radioactive material and associated facilities and activities, and material out of regulatory control, as well as to account for terminology that has evolved within the IAEA Nuclear Security Series.

Since the initial drafting of NSS No. 23-G and in response to the rapid development and use of digital technologies and computer based systems in nuclear applications, accompanied by rapidly evolving adversary tactics, techniques, and procedures, the content and concepts contained in the current NSS No. 23-G warrant review and revision. Notably, since its publication, additional good practices within national approaches are being implemented to address vulnerabilities for establishing and sustaining information security management systems, which merit review and possible inclusion.

This revision will aim to update the guidance on information security protection applied to sensitive information, information assets and digital assets, ensuring the preservation of confidentiality, integrity, and availability, as well as applicability across the topics covered within the Nuclear Security Recommendations.

4. OBJECTIVE

This publication will provide guidance on implementing the principles of information security including maintaining the confidentiality, integrity, and availability of information to support the establishment and maintenance of information security programmes for nuclear security. Much national and international guidance exists regarding the establishment and management of information security frameworks for information of various types, in the form of both high level guidance and detailed standards. This publication does not intend to replace such guidance. Instead, its goal is to assist States in bridging the gap between existing government and industry standards on information security in general, the particular concepts and considerations that apply to nuclear security, and the special provisions and conditions that exist when dealing with nuclear material and other radioactive material.

This Implementing Guide is intended for policy makers, competent authorities, operators, shippers, carriers and others with responsibilities for the creation, storage, and use of sensitive information relevant to nuclear security and safety.

5. SCOPE

The guidance in this publication applies to information security for nuclear security relating to elements of a State’s nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, and the detection of and response to nuclear security events. This Implementing Guide will also address information security related to nuclear material accountancy and control and nuclear and other radioactive material in transport, as well as the interfaces of information security for nuclear security with nuclear safety.

This publication refers to guidance on the security of the subset of sensitive information assets that are also digital assets (i.e. computer based systems) as referred to in the Nuclear Security Fundamentals NSS No. 20 and the Nuclear Security Recommendations Nos 13, 14 and 15, but detailed guidance on this topic is excluded from the scope. NSS No. 42-G provides guidance on the computer security aspects of computer based systems, the compromise of which could adversely affect nuclear security and/or nuclear safety.

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

The proposed publication will be an Implementing Guide in the IAEA Nuclear Security Series. It will reside under, and interface with, the following IAEA Nuclear Security Series publications:

- 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).
- INTERNATIONAL ATOMIC ENERGY AGENCY, 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, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021)
- 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, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021)
-

Interfaces with safety may include at least the following IAEA publications:

- INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).
- INTERNATIONAL ATOMIC ENERGY AGENCY, Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency, Emergency Preparedness and Response Series, revision of EPR-METHOD (2003) (in preparation).
- FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

7. OVERVIEW

A proposed table of contents for the draft is as follows, including proposed updates:

1. INTRODUCTION
    - Background, Objective, Scope, Structure.

2. CONCEPTS AND CONTEXT
    - This section would be substantially expanded to support the description of computer security as a proper subset of information security. It would further expand on the context of sensitive information and sensitive information assets to span activities occurring across an entire nuclear security regime, including sensitive information maintained by non-state entities, in alignment with the revised scope of the publication.
3. FRAMEWORK FOR SECURING SENSITIVE INFORMATION
    - This section would ensure application across a nuclear security regime and introduce further considerations to ensure the management framework coverage of integrity and availability in addition to the current coverage of confidentiality. This may be discussed in terms of the importance of implementing the national framework with a risk management perspective.
4. IDENTIFYING SENSITIVE INFORMATION
    - This section would provide a greater degree of coverage for all areas where sensitive information may exist within a nuclear security regime.
5. ACCESSING, HANDLING, SHARING, AND DISCLOSING SENSITIVE INFORMATION
6. MANAGEMENT FRAMEWORKS FOR CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY
    - This section would be expanded to ensure the guidance represents integrity and availability of information in addition to confidentiality.

REFERENCES

ANNEXES

GLOSSARY

8. PRODUCTION SCHEDULE:

	B*
STEP 1: Preparing a DPP	DONE
STEP 2: Internal review of the DPP (Approval by the Coordination Committee)	Q1 2022
STEP 3: Review of the DPP by the review Committee(s) (Approval by review Committee(s))	Q2 2022
STEP 4: Review of the DPP by the CSS (approval by CSS) or information of the CSS on the DPP	
STEP 5: Preparing the draft publication	Q3 2022
STEP 6: First internal review of the draft publication(Approval by the Coordination Committee)	Q1 2024
STEP 7: First review of the draft publication by the review Committee(s) (Approval for submission to Member States for comments)	Q2 2024
STEP 8: Soliciting comments by Member States	Q3 2024
STEP 9: Addressing comments by Member States	Q4 2024
STEP 10: Second internal review of the draft publication (Approval by the Coordination Committee)	Q1 2025
STEP 11: Second review of the draft publication by the review Committee(s) (Approval of the draft)	Q2 2025
STEP 12: (For Safety Standards) Editing of the draft publication in MTCD and endorsement of the draft publication by the CSS	Q3 2025

(For nuclear security guidance) DDG's decision on whether additional consultation is needed, establishment by the Publications Committee and editing	
STEP 13: Approval by the Board of Governors (for SF and SR only)	
STEP 14: Target publication date	2026

9. RESOURCES

It is estimated that the development of this Implementing Guide would involve approximately 36 weeks of effort by Member States' experts. This is based upon assuming 3 one-week expert meetings involving about an average of 8 experts, and an average of 2 weeks of work per expert between meetings. Secretariat resources involved are estimated at 16 weeks of effort by agency staff and assisting resources plus support for expert travel and honoraria for experts whose effort is not otherwise funded.