Document Preparation Profile (DPP)

Version 1 02/05/2025

1. IDENTIFICATION

Nuclear Security Technical Guidance

Working ID:	**NST076**
Proposed Title:	**Computer Security of Operational Technologies and Instrumentation and Control Systems for Nuclear Security**
Proposed Action:	**Revision of a publication Computer Security of Instrumentation and Control Systems at Nuclear Facilities, 2018, NSS No. 33-T**
Review Committee(s) or Group:	**NSGC, NUSSC, EPReSC, RASSC, TRANSC, WASSC**
Technical Officer(s):	**Trent NELSON**

2. BACKGROUND

The Nuclear Security Series (NSS) No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, was published in 2018 to address the application of computer security controls to Instrumentation and Control (I&C) systems at nuclear facilities. The document provides guidance directly related to the computer security of nuclear materials, but also examines considerations for computer security of nuclear safety systems, and the potential implications of computer security controls on such systems. Since then, two new computer security publications have been released: NSS No. 42-G, Computer Security for Nuclear Security, and NSS No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities, were published in 2021. These publications introduced updated computer security frameworks and techniques that need to be incorporated into the revision of NSS No. 33-T.

This is important because Operational Technology (OT) systems, including I&C systems, are the foundation of many nuclear safety and security systems used in operations and nuclear facilities.

NSS No. 33-T also interfaces with several safety and security guidance publications that have undergone revisions since its publication. Some additional new concepts, like cyber-by-design, have also been developed that need to be taken into account during the revision of NSS No. 33-T.

3. JUSTIFICATION FOR THE UPDATE OF THE DOCUMENT

Currently, NSS No. 33-T is not aligned with the more recent computer security NSS publications such as those listed below, and it has also gaps, which are detailed in the annex:

- NSS No. 42-G, Computer Security for Nuclear Security, published in 2021.
- NSS No. 23-G, Security of Nuclear Information, currently in the last steps on its first revision.
- NSS No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities, published in 2021.

Additionally, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, is currently under review and Specific Safety Guide SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants, is scheduled for review in 2026.

Due to the release of newer computer security publications and the advancements of digital technologies (advanced control technologies), NSS No. 33-T requires an update to ensure consistency with the NSS publications and to provide comprehensive guidance across all the nuclear security domains that use I&C systems.

4. OBJECTIVE

The objective of the revision is to provide cross-cutting guidance on computer security controls and measures for I&C systems within OT environments that control and support nuclear security and nuclear safety related functions.

The revision will provide up-to-date guidance on computer security measures across various domains, including interactions with cloud-based systems, facility lifetimes (from design to decommissioning), component lifecycle management, and human component of the OT systems. Additionally, informative annexes including worked examples and references to other relevant publications will offer practical insights and support on computer security for OT systems.

While the primary focus of this publication is on the secure operation of digital systems, it also has the potential to contribute to enhance safety and operational performance of nuclear facilities.

This revised guidance is intended for all parties involved in the design, operation, and regulation of nuclear facilities, including competent authorities, regulatory bodies, designers, license applicants, facility personnel (e.g., operations, maintenance and engineering personnel), vendors, contractors and suppliers, research laboratories.

5. SCOPE

The primary scope of this revision focuses on the application of computer security measures to OT systems in nuclear facilities. These systems perform critical functions, including security, safety, and auxiliary operations, at facilities that use, store, and transport nuclear material and other radioactive material. Additionally, the revision covers OT systems that monitor the retrieval of material outside of regulatory control.

This revision will be aligned with the three-recommendation level publications of the NSS (NSS Nos 13, 14, and 15) that are currently under revision. The revision also addresses the application of computer security measures to the development, simulation, and maintenance environments of OT systems.

The revision will also examine the security implications of introducing emerging digital technologies, such as autonomous, remote operation, wireless, cloud computing, and artificial intelligence, as well as the implementation of a zero-trust model for OT systems. This will help strengthen security in order to mitigate potential weaknesses in OT systems.

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

The proposed publication will interface with the following:

- NSS Fundamentals and Recommendations:

  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)

- NSS Implementing Guides and Technical Guidance:

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

INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

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)

INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).

- Safety Standards:

INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standard, Specific Safety Requirements No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016)

INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standard, Specific Safety Guide. No. SSG-39, IAEA, Vienna (2016)

INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standard, General Safety Requirements No. GSR part 7, IAEA, Vienna (2015)

7. OVERVIEW

INTRODUCTION

Background
Objective
Scope
Structure

CONCEPTS AND RELATIONSHIPS FOR COMPUTER SECURITY OF OPERATIONAL TECHNOLOGY SYSTEMS

Multi-disciplinary relationships
Summary of related documents
Functions, consequences and the Graded Approach
Computer security of OT systems

Computer security measures
Secure by Design and an engineering approach
How to manage the risk with emerging digital technologies

LIFECYCLES RELEVANT TO COMPUTER SECURITY OF OPERATIONAL TECHNOLOGY SYSTEMS

Facility lifecycles (lifetime) including design maturity, licensee phases, SSR 2/1
System lifecycle that lines up with SSG-39… Safety–security interfaces
Lifecycle for I&C
Lifecycle of other OT systems (outside I&C)

CROSS-CUTTING GUIDANCE FOR COMPUTER SECURITY OF I&C SYSTEMS WITHIN OPERATIONAL TECHNOLOGY

Protecting functions (e.g., control I&C, security and safety related functions)
Guidance common to all lifecycle phases
Guidance for specific lifecycle phases
Guidance for specific functions (like Emergency Preparedness & Response)

ADDITIONAL GUIDANCE SPECIFIC TO NUCLEAR FACILITIES OPERATIONAL TECHNOLOGY

ADDITIONAL GUIDANCE SPECIFIC TO PHYSICAL PROTECTION SYSTEMS OPERATIONAL TECHNOLOGY

ADDITIONAL GUIDANCE SPECIFIC TO NUCLEAR MATERIAL ACCOUNTANCY OPERATIONAL TECHNOLOGY

ADDITIONAL GUIDANCE SPECIFIC TO RADIOACTIVE MATERIALS OPERATIONAL TECHNOLOGY

ADDITIONAL GUIDANCE SPECIFIC TO MATERIAL OUTSIDE OF REGULATORY CONTROL OPERATIONAL TECHNOLOGY

ANNEXES

OT and I&C for Small Modular Reactors
Defensive Computer Security Architecture (DCSA) for Physical Protection Systems
DCSA for Nuclear Material Accountancy and Control

8. PRODUCTION SCHEDULE:

Provisional schedule for preparation of the document, outlining realistic expected dates for (f*ill the column corresponding to your proposed document and delete the other columns*):

STEP 1: Preparing a DPP	DONE
STEP 2: Internal review of the DPP (Approval by the Coordination Committee)	July/Aug. 2025
STEP 3: Review of the DPP by the review Committee(s) (Approval by review Committee(s))	December 2025
STEP 4: Information of the CSS on the DPP	March 2026
STEP 5: Preparing the draft publication	Q1/Q4 2026
STEP 6: First internal review of the draft publication (Approval by the Coordination Committee)	Q1 2027
STEP 7: First review of the draft publication by the review Committee(s) (Approval for submission to Member States for comments)	Q2 2027
STEP 8: Soliciting comments by Member States	Q3/Q4 2027
STEP 9: Addressing comments by Member States	Q1 2028
STEP 10: Second internal review of the draft publication (Approval by the Coordination Committee)	Q1 2028

STEP 11: Second review of the draft publication by the review Committee(s) (Approval of the draft)	Q2 2028
STEP 12: DDG's decision on whether additional consultation is needed, establishment by the Publications Committee and editing	Q3 2028
STEP 14: Target publication date	Q1/Q2 2029

9. RESOURCES

Estimated resources involved by the Secretariat (person-weeks) and the Member States (number and type of meetings)

Staff resources

NSNS – 1 TO 10 weeks

Meetings 4 CM before step 7, 1 CM before step 11.

Home Based Assignments (as appropriate)

Annex to the DPP for a revision of NSS No 33-T

Gap analysis

Short recall

Two implementing guides (NSS 23-G and NSS 42-G) and two Technical Guidance (NSS 17-T Rev. 1 and NSS 33-T), provide the basis for information and computer security, offering more details on some fundamental elements of NSS 20, as well as recommendation level guidance in NSS 13, NSS 14 and NSS 15, and at least, SSR 2/1 and SSG-39 for nuclear safety.

Needs expression during IAEA events

The 2022 *Technical Meeting on Instrumentation and Control, and Computer Security for Small Modular Reactors and Microreactors*, the 2023 *International Workshop on Instrumentation and Control, and Computer Security for Small Modular Reactors* and the *CyberCon23* emphasized the importance to revise NSS 33-T due to inconsistencies with newer publications and the limitation of a direct focus on nuclear facilities. It is proposed this document should be a cross-cutting publication supporting all nuclear security domains including addressing emerging digital technologies, machine learning, Artificial Intelligence and Small Modular Reactors and Microreactors.

Informing a potential revision

To address the gap analysis, and support a potential revision of the NSS 33-T a consultancy meeting was held from 2 to 6 Sept. 2024 in which the invited experts provided detailed justification as follows:

- Inconsistencies in NSS 33-T due to parallel development of IAEA documents and newer publications and updates:
    - NSS 33-T was written in parallel of SSG 39 (which derives from SSR 2/1) and before the first version of NSS 17-T.
    - The new NSS 42-G and NSS 17-T (Rev 1) were since written and published in 2021, and the first revision of NSS 23-G has been drafted and in the final Steps for publication.
- As a result of this, NSS 33-T effectively presents overlaps or inconsistencies with other IAEA guidance.

  Further, in parallel of the evolution of the IAEA guidance, computer security approaches within other standards (such as IEC, ISO and other documents) are overlapping the original NSS 33-T that does not go into the same level of technical details.
- About safety/security interface:

  The revised NSS 33-T document could provide guidance on how to strengthen and actively manage the interface between safety and the protection of OT (Operational Technologies, i.e., linked to I&C) systems, from initial design, through operation, to decommissioning. This would provide useful inputs for the revision of other documents to come, like the planned revision of SSR 2/1 and SSG-39.

  Further, guidance on certain aspects of the safety interfaces with security need to be clarified, improved and updated in order to reflect the best practices developed since the initial development of NSS 33-T.
- About emerging technologies:

  Technology is accelerating and new technology such as SMR, Microreactors, Artificial Intelligence, cloud computing, and remote operations and maintenance should be considered on the impact of computer security for I&C systems.

Since OT is distinguished from Information Technologies (IT) for business activities, the boundary between both technologies is merging and OT may include IT-like platforms or in the near future Cloud based systems.

Currently, NSS 33-T doesn't include these new approaches, which need to consider security-by-design and emerging technology impacts.

- About human interaction:

  OT have to be understood as computer-based digital technologies that control real-world processes. In this way, OT includes but are not limited to I&C (Industrial Control) systems. Therefore, OT also includes the human actions as a part of the systems, which should be considered in this revision.

- About the scope:

  The original scope of NSS 33-T was focused on nuclear power plants. As the computer security for nuclear activities may be needed in other areas of the nuclear security regime, the scope of the document should cover all the Nuclear Security domains (e.g., NMAC, PPS, EP, SSS, Rad and MORC).

Example of topics that may be explored in a NSS 33-T revision:

- Clarification of the relationship between computer security and safety.
- Baseline computer security requirements for SMR.
- Practical development on function defence, data-flows and trust relationships complementing NSS No. 17-T (rev.1).
- Clarification of the lifecycle concepts.
- Practical guidance on supply chain issues.
- Consideration and possible guidance on implementing OT-SOCs (Security Operation Centres) and on their relationship with other security components (Central Alarm Station, Main Control Room, IT SOC, Incident and safety Event Response…).
- Clarification of the concept of SDA (Sensitive Digital Asset) in order to better focus on function protection rather than on assets security.
- Clarification of the concept of DBT (Design Basis Threat) for computer security.