Computer Security of Operational Technologies and
Instrumentation and Control Systems for Nuclear Security (NST076 – DPP for revision of NSS 33-T)

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
1.	Title *Reviewer: C. Martin (ENISS)*	Computer Security of Operational Technologies ~~and~~ including Instrumentation and Control Systems for Nuclear Security	I&C is a part of OT systems and not different from OT (as mentioned in section 2)	X			
2.	General *Reviewer: Bartosz Szwaj (PAA, Poland)*	Consider adding the topic of obsolescence of I&C workstations operating systems and guidance how to treat them.	Control system and other vendors provide much shorter support time for their products than the lifetime of a facility. In practice many facilities have obsolete operating systems, such as for example Win 3.11. Maybe it will be good to provide guidance how to manage obsolescence.	X			
3.	General *Reviewer: Ross Obuchi (CNSC, Canada)*	The scope of revision is ambitious. While guidance is needed for OT, as well as I&C, the scope of consensus guidance development across a wide range of facilities may be difficult.	To date, consensus implementing guidance related to computer security has been for nuclear facilities and nuclear material. It could be challenging to identify contributors in other areas (ORM and MORC), and even more challenging to reach consensus.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			Therefore, the Production Schedule for drafting throughout 2026 may need to be lengthened, depending on expert availability.				
4.	General *Reviewer: Ross Obuchi (CNSC, Canada)*	Following comment #1, above, a proposal could be to maintain the wide scope of this document, but create implementing guide for different types of facilities and materials.	Example could be one IG for nuclear facilities, one for radioactive materials, and one for MORC to align with NSS 13, 14 and 15.	X			
5.	General *Reviewer: S. Marogulov (State Corporation Rosatom, Russian Federation)*	Avoid extensive investigation of interface with safety during development of the document.	In the DPP, much emphasis is put on the benefits of computer security for nuclear safety. Though it is true, this is not a safety document and such emphasis is of little use for nuclear security specialists. The revision should not shift the focus of the document to the safety-security interface and should stay within the boundaries of nuclear security, with acknowledgement of points of interface with safety.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
6.	2. BACK-GROUND/L4 *Reviewer: Haruyuki Ogino (Nuclear Regulation Authority, Japan)*	The document provides guidance directly related to the computer security of physical protection system and nuclear materials accountancy and control system, but also examines considerations for computer security of nuclear safety systems, and the potential implications of computer security controls on such systems.	Clarification The term "computer security" is used for the systems, not material, so conform to the footnote no.3 of NS 33-T (2018), "Systems providing security functions include those used for physical protection and nuclear material accountancy and control." .		X "The document provides guidance directly related to the computer security of nuclear facilities, including considerations for computer security of nuclear safety-related systems,~~co mputer security of security-related functions of nuclear facilities~~"		

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
7.	Section 3 *Reviewer: C. Martin (ENISS)*	Use only the term OT in all the text	The terms I&C and OT are not used consistently throughout the document (for instance, I&C is used at the end of Section 3, whereas Section only use OT). Consistency check seems needed.	X			
8.	Section 3 *Reviewer: C. Martin (ENISS)*	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~~ OT systems.	Not only I&C systems but OT systems as a whole	X			
9.	(Chap. 3) and the advancements of digital technologies (advanced control technologies), *Reviewer: Brice DELIME (France)*	and the advancements of digital technologies,	what does “advanced control technologies” means ? Proposition to remove this notion.	X			
10.	*Reviewer: Brice DELIME (France)*	(Chap 3) NSS 33-T effectively presents overlaps or inconsistencies with other IAEA guidance. Further,	To be added (in chap 3, chap 6 or annex) : Coordination between IEC work on nuclear			X	Despite the importance of coordinating and

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		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. It would be beneficial to mention the need for coordination between IEC work on nuclear I&C system cybersecurity (in particular with the revision of IEC 62645) and NSS 33-T revision. It would be consistent with the existing agreement between IAEA and IEC on nuclear security.	I&C system cybersecurity (in particular with the short term revision of IEC 62645) and NSS 33-T revision would be valuable.				consistence with other standards such as IEC, ISO, etc, direct reference to specific documents may lead to obsolescence of the document depending on the evoltio
11.	Section 4 *Reviewer: C. Martin (ENISS)*	The objective of the revision is to provide cross-cutting guidance on computer security controls and measures for OT systems ~~I&C systems within OT environments~~ that control and support nuclear security and nuclear safety related functions	Idem	X			
12.	Section 4 *Reviewer: C. Martin (ENISS)*	The revision will provide up-to-date guidance on computer security measures taking into account ~~across various domains, including~~	Proposal of a new formulation to be clearer		X The revision will provide		

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		interactions with cloud-based systems, new and emerging technologies (AI, IoT,…), 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.			up-to-date guidance on computer security measures taking into account new and emerging technologies,~~Not giving examples of new technologies to preserve~~"		
13.	Section 4, para 3 *Reviewer: Paula Karhu (STUK, Finland)*	Add text: "The guidance will promote a risk-informed approach to ensure proportionality and effectiveness of security measures throughout a system's lifecycle. It will support integration/coordination of computer security with physical protection and safety, contributing to a holistic and balanced approach to nuclear security.	For effectiveness, comprehensiveness, and interface management. In line with the annex of the DPP.		X No direct reference to ISO 27k family of standards		

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		To ensure relevance and applicability, the guidance will be harmonized with relevant existing international standards (such as ISO/IEC 27 000 standards family) and frameworks. It will promote continuous improvement through feedback mechanisms, incident analysis, and lessons learned, and facilitate international collaboration and sharing of good practices among stakeholders." or equivalent					
14.	(Chap 4) 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. *Reviewer: Brice DELIME (France)*	4. OBJECTIVE The objective of the revision is to provide cross-cutting guidance on computer security controls and measures for OT systems, including I&C systems, that control and support nuclear security and nuclear safety related functions.	OT should be defined first. The scope of the NSS 33-T is broader than I&C systems as stated in the chapter objectives: "The primary scope of this revision focuses on the application of computer security measures to OT systems in nuclear facilities."	X			
15.	Section 5, para 3 *Reviewer: Paula Karhu (STUK, Finland)*	Add: "The revision will also examine the security implications of introducing emerging digital technologies, such as autonomous,	For comprehensiveness. In line with the annex to the DPP.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		remote operation, wireless, cloud computing, and artificial intelligence, as well as the implementation of a zero-trust model for OT systems, including insider threat mitigation and supply chain security."					
16.	Section 5 *Reviewer: Paula Karhu (STUK, Finland)*	Add text: "The scope includes the entire lifecycle of the facility and the OT systems, from design and deployment to decommissioning, and considers the human and organizational factors affecting the security of OT systems. It includes the interfaces between OT and IT systems, addressing potential threats, vulnerabilities and integration challenges." Consider adding: "The scope includes a wide range of nuclear facilities, including power reactors, research reactors, SMRs, storage sites, and transport operations, as appropriate".	In line with section 4 and the annex to the DPP.	X			
17.	(Chap. 5) The revision also addresses the application of computer security	The revision also addresses the application of computer security measures to the development, V&V,	Proposition to take into account the potential dedicated environment for		X "verification and		Putting only the abbreviation of V&V would not be clear to all readers.

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	measures to the development, simulation, and maintenance environments of OT systems. *Reviewer: Brice DELIME (France)*	simulation, and maintenance environments of OT systems.	verification and validation purpose.		validation (V&V)"		
18.	(Chap. 5) emerging digital technologies, such as autonomous, remote operation, wireless, cloud computing, and artificial intelligence *Reviewer: Brice DELIME (France)*	emerging digital technologies, such as autonomous, remote operation, smart sensors / IIoT, wireless, cloud computing, artificial intelligence	Smart sensors / Industrial Internet of Things could lead to its own potential weaknesses.		X "smart sensors / Industrial Internet of Things (IIoT)"		Putting only the abbreviation of IIoT would not be clear to all readers.
19.	(Chap5): 5. SCOPE: 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	In order to provide relevant guidance, 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.	The objective of a NSS Technical Guidance is to produce considerations and guidance.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	order to mitigate potential weaknesses in OT systems. *Reviewer: Brice DELIME (France)*						
20.	5 (Scope) *Reviewer: Ross Obuchi (CNSC, Canada)*	Care may need to be practised in order to properly scope computer security, particularly for MORC applications.	MORC represents a unique situation, without a dedicated responsible operator. It is unclear who would be responsible for implementing computer security, and for what purpose(s).	X			
21.	5/20 *Reviewer: Bartosz Szwaj (PAA, Poland)*	(…) wireless, cloud computing, **virtualization,** and artificial intelligence (…)	Control system vendors can now also provide virtualization, thus considerations regarding virtual machines and VLANs should be included.	X			
22.	6. PLACE IN THE OVERALL STRUCTURE OF THE RELEVANT SERIES AND INTERFACES WITH EXISTING AND/OR PLANNED PUBLICATIONS *Reviewer: S. Marogulov (State Corporation*	Add IAEA document NSS No. 8-G	Insider with cyber-skills is described in NSS 8-G. Therefore NSS 8-G and approaches of computer's insider tactics and countermeasures against them are connected with NST076. Also NST076 is a technical guidance, so specific details about computer's insider from NSS	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	Rosatom, Russian Federation)		8-G are logical to be considered.				
23.	Section 7 *Reviewer: C. Martin (ENISS)*	Integrate the text of the part "additional guidance specific to nuclear facilities OT" in the main text to make sure that DPP concerns OT above all (I&C is a part of OT systems).	In Section 7 (overview) the DPP provides a preliminary structure. There's a part called "Additional guidance specific to nuclear facilities OT. This is confusing, as it may involve that OT is not englobing I&C, for which guidance are provided just before. The articulation with the other additional guidance part is also unclear.	X			
24.	Section 7 *Reviewer: Paula Karhu (STUK, Finland)*	Consider mentioning the interfaces of human factors and technology, IT and OT, safety and security.	In line with other sections, the annex to the DPP, and "Multi-disciplinary relationships" in section 7.	X			
25.	7. OVERVIEW *Reviewer: S. Marogulov (State Corporation Rosatom, Russian Federation)*	CONCEPTS AND RELATIONSHIPS FOR COMPUTER SECURITY OF OPERATIONAL TECHNOLOGY SYSTEMS Multi-disciplinary relationships	The Secretariat should provide additional clarification, what will be included under this sub-section. The original document seemed to have no such sub-section, and it doesn't align with the justification for the revision.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
26.	7. OVERVIEW *Reviewer: S. Marogulov (State Corporation Rosatom, Russian Federation)*	CROSS-CUTTING GUIDANCE FOR COMPUTER SECURITY OF I&C SYSTEMS WITHIN OPERATIONAL TECHNOLOGY	The entire chapter is dedicated to interface with safety. This does not correspond with justification for the revision and this is not an interface and/or cross-cutting document, thus the addition of an entire chapter for this topic is excessive. The information should be included in other sections as appropriate and to the extent it is crucial for nuclear security purposes.	X			
27.	7. OVERVIEW *Reviewer: S. Marogulov (State Corporation Rosatom, Russian Federation)*	ADDITIONAL GUIDANCE SPECIFIC TO…	The logic behind the division of these chapters is unclear (it mixes facilities, physical protection, different types of material, NMAC and MORC). Additional clarification is required.	X			
28.	7. OVERVIEW *Reviewer: S. Marogulov (State Corporation Rosatom, Russian Federation)*	ADDITIONAL GUIDANCE SPECIFIC TO NUCLEAR MATERIAL ACCOUNTANCY OPERATIONAL TECHNOLOGY	The addition of NMAC into this list is questionable, as NMAC is a separate branch, which is considered as such in the existing version of the NSS 33-T. It is suggested to delete a separate chapter dedicated to it and include	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			the information into other chapters as appropriate and to the extent needed for nuclear security purposes.				
29.	Annex *Reviewer: C. Martin (ENISS)*	Term OT to be defined	The term OT should be defined in the frame of this document as it is not defined in the IAEA glossary (the DPP annex provides a general definition though)	X			
30.	Annex Page 6 Line 36 New issue *Reviewer: Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN) (with comments of GRS), Germany*	• About emerging technologies: Technology is accelerating and new technology such as SMR, Microreactors, Artificial Intelligence ~~,~~and cloud computing ~~and remote operations and maintenance~~ should be considered on the impact of computer security for I&C systems. • About outsourcing: Remote operations, monitoring, inspection and maintenance, off-premises data handling and storage, and increasing dependency on external personnel should be considered on the impact of computer security for I&C systems.	Remote operations and maintenance is not so much an aspect of emerging technologies, but of outsourcing of work, allowing for additional data connections, increasing dependency on external computer systems and external personnel. Quite similar are remote monitoring and inspection as well as off-premise data handling and storage. Examples could include Security Operations Center (SOC) and Security Information and Event Management (SIEM). Therefore, we recommend an	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			additional bullet point for this aspect.				
31.	Annex Page 7 Line 7 *Reviewer: Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN) (with comments of GRS), Germany*	In this way, OT includes but ~~are~~ is not limited to I&C ~~(Industrial Control)~~ systems.	1) There seems to be a typo. 2) Abbreviation I&C – as Instrumentation and Control - is introduced in text before.	X			
32.	Annex Page 7 Line 13 *Reviewer: Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN) (with comments of GRS), Germany*	… the scope of the document should cover all the Nuclear Security domains including ~~(e.g.,~~ NMAC, PPS, EP, SSS, Rad, ~~and~~ MORC and security of nuclear materials in transport~~)~~**.**	As so many domains are named explicitly, transport should be amongst them. Also, the domains are important and should therefore not be placed in brackets. Additionally, please consider the possibility to clarify the meaning of these abbreviations, allowing for a more reader friendly document, such as “Nuclear Material Accounting and Control (NMAC)” instead of simply “NMAC”.	X			
33.	Annex, Page 7 Line 20	Practical guidance on reducing cyber risks in the supply chain ~~issues~~.	The focus should be clearly on reducing the cyber risks.	X			

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	Reviewer: Federal Ministry for the Environment, Climate Action, Nature Conservation and Nuclear Safety (BMUKN) (with comments of GRS), Germany						
34.	Annex, page 7 *Reviewer: C. Martin (ENISS)*	Example of topics that may be explored in a NSS 33-T revision: ….. 1. Threat Intelligence & Sharing Recommendation: Incorporate guidance on integrating threat intelligence platforms (e.g., MITRE ATT&CK, STIX/TAXII) and establishing mechanisms for sharing threat data across nuclear facilities and with national/international partners. 2. Behavioral Monitoring & Anomaly Detection Recommendation: Introduce AI/ML-based behavioral analytics for detecting anomalies in OT systems, enhancing detection of insider threats and advanced persistent threats. 3. Red/Blue/Purple Teaming Practices	This supplement proposes the inclusion of additional cybersecurity topics in the upcoming revision of NSS 33-T, based on current trends and identified gaps in the draft document.		X, included only the titles, for consistence with the other bullets in the section.		

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		Recommendation: Encourage adversary emulation exercises, penetration testing, and tabletop simulations tailored to OT environments to validate resilience and response capabilities. 4. Post-Quantum Cryptography Considerations Recommendation: Include awareness and planning for post-quantum cryptographic algorithms in long-lifecycle OT systems to ensure future-proofing against quantum threats. 5. Governance, Risk & Compliance (GRC) Frameworks Recommendation: Map technical controls to strategic GRC frameworks (e.g., ISO/IEC 27005, NIST CSF, COBIT) to support regulatory compliance and risk-based decision-making in OT environments. 6. Mobile Device & BYOD Security Recommendation: Address policies and controls for mobile access to OT systems, including BYOD restrictions and secure remote access protocols.					

COMMENTS BY REVIEWER Reviewer: Page.... of.... Country/Organization: Date: **28 Oct 2025**				RESOLUTION			
Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		7. Cyber Resilience Principles Recommendation: Embed resilience concepts (e.g., NIST SP 800-160 Vol. 2) into OT system design and operations to ensure continuity and recovery in the face of cyber disruptions.					