Comment Code	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
CAN.3	Canada		3	1.1	Provide reference to Confidentiality, Integrity and Availability of information Reference to NSS 42-G Para 1.3 "The security of sensitive information and sensitive information assets implies protecting the confidentiality, integrity and availability of such information and assets."	The focus on confidentiality is too limiting and does not align with the definition of sensitive information ("Information, in whatever form, including software, the **unauthorized disclosure, modification, alteration, destruction, or denial of use** of which could compromise nuclear security")	X	NSS 20-F does not cover integrity and avaliability but is the authoratative higher level basis in the NSS and should still be referenced. Added as 1.8 but still within background. Adapted into a new paragraph 1.3 the CPPNM reference from NSS 42-G Para 1.3 (previously [8]) and the dangling reference to ICSANT (previously [9]).		
CAN.4	Canada		4	1.2	Switch order with clause 1.1	This is a much better global sentence regarding the objectives of protecting sensitive information (clause 1.1 is limited to information confidentiality)	X			
DEU.1	Germany	Germany/Technical University Munich, FRM II	1	1.4	"IAEA Nuclear Security Series Nos 13, … [3]; 14, … [4]. and 15, … [5] provide recommendations on the protection of sensitive information."	Minor editorial correction: removal of a surplus punctuation mark after reference number '[4]'.	X			
PAK.3	Pakistan	PAEC	3	1.5	Following text may be included:Groups or individuals wishing to plan or commit a criminal or other intentional unauthorized act involving nuclear material or other radioactive material or associated facilities could benefit from acquiring, modifying or denying access to sensitive information.Sensitive information is "information, in whatever form,	Databases related to capacity building, personal reliability and trustworthiness program. Record of modifications, maintenance record may contain sensitive information, therefore, may be includedTo conform with Para 2.31			X	This cannot be accepted as it would be modifying a quote from an existing publication, in section 1 these are just provided as background. A better definition can be considered in a revision of the NS Glossary and then promulgated.

					including software, databases, the unauthorizeddisclosure, modification, alteration, destruction, or denial of use of which could compromisenuclear security					
PAK.1	Pakistan	PNRA	1	1.5	Groups or individuals wishing to plan or commit a criminal or other intentional unauthorized act involving nuclear material or other radioactive material or associated facilities **and activities** could benefit from acquiring, modifying or denying access to sensitive information.	For harmonization of the text throughout the document, the additional highlighted wording may be considered to make the text in line with the scope (paragraph 1.13, 1.14) and paragraph 1.1 of the subject draft NST070.	X			
FIN.2	Finland	Paula Karhu	2	Para 1.5	Consider the definition quoted from ref. [2]: whether both “modification” and “alteration” are needed.	For clarity. Alternatively, the difference between modification and alteration could be explained.			X	This is quoted from the IAEA NS Glossary, the quote cannot be modified in an implementing guide per SPESS C. A recommendation will be made to the responsible technical officers for terminology to consider both terms or if it can be reduced to a single term. To support this harmonisation terms in this document will be normalised to "modification" including "alteration" and "manipulation".

FIN.3	Finland	Paula Karhu	3	Para 1.5	Add the words "or safety" at the end of the para.	For ensuring information availability for safety purposes – there could be a case of non-availability that would not compromise security but could compromise safety (e.g. in a "pure" accident management situation without security threat).	X	This is quoted from the IAEA NS Glossary. A recommendation will be made to the responsible technical officers for terminology to expand the applicability but as it's a quote the current version will remain in the draft until the glossary can be addressed. However during drafting this was considered which is why the next paragraph talks about "nuclear security and it's interfaces with nuclear safety". An expansion of this wording has been proposed to make this more evident to the reader.		
FIN.4	Finland	Paula Karhu	4	Para 1.6 and the following.	Modify: "…This Implementing Guide provides guidance on information security for nuclear security and its interfaces with nuclear safety.	Ensuring integrity and availability are very much in the interests of nuclear safety. And they are part of information security. Same as comment 1.			X	The DPP is approved with a scope of information security for nuclear security. Efforts have been made within the document to address the interfaces with nuclear safety i.e. protecting the performance of nuclear safety functions against criminal and other intentional unauthorised acts but that is the limit of the scope. The guidance within the publication equally might not fully

										address all information security concerns in the safety domain, for instance the need for redundancy of technologies to correct errors in information resulting from natural phenonmena rather than a malicious act (e.g. mechanically failing hard drives or bitflipping of random access memory on a computer).
PAK.2	Pakistan	PNRA	2	1.7	Some sensitive information is **created,** controlled, stored, processed or communicated through computer-based systems (i.e. sensitive digital assets).	For the sake of completion of life cycle of information and to make the paragraph in line with section 5 (Lifecycle of Sensitive Information), the additional highlighted wording is proposed, please.	X			
FIN.5	Finland	Paula Karhu	5	Para 1.7 (or 2.30 for example)	Consider adding: "In computer security information technology (IT) and operational technology (OT) systems often require a different emphasis and balance between the confidentiality, integrity, and availability domains."	Or similar text, to raise awareness of the differences of the two environments and the related risks and possibilities to implement the "CIA".	X	The distinction on how CIA is managed in IT compared to OT belongs in NSS 42-G and is not within the scope of NSS 23-G. To highlight the applicablity of NSS 42-G to both IT and OT a footnote has been added to clarify the scope of NSS 42-G aligned with specifying OT and IT. A footnote was suggested rather than body text due to not attributing or binding a different scope for NSS 42-G within guidance		

								statements in NSS 23-G.		
CAN.5	Canada		5	1.8	Document should contain its own glossary of key terms.	For key terms – it may be helpful to repeat them in this document's glossary as they may change.			X	Per SPESS C there are no definitions in implementing guides or technical guidance. Definitions are in the NS glossary or in higher level publications, relevant terms reflect their use in the above.
DEU.2	Germany	Germany/Technical University Munich, FRM II	2	1.8	"The terms used in this publication are to be understood as explained in the IAEA Nuclear Safety and Security Glossary [2], unless otherwise stated in the text."	Citation of the correct title of the IAEA Nuclear Safety and Security Glossary in the text.	X			
CAN.6	Canada		6	1.9	Remove this clause	This document may be Rev 1 of NSS 23-G			X	This is the standard format clause for revisions of IAEA publications highlighting the document will indeed be published as Rev 1 of NSS 23-G.
CAN.10	Canada		10	Section 2Information Security Concepts	This section introduces terms such as "information object" and "information asset" that could be replaced with "sensitive information" with no impact to the meaning of the document while enhancing clarity.				X	The terms are not introduced in the section, they are defined by precedent and used throughout the NSS. There are distinctions that have been established and NST070 has been drafted to provide greater clarity.

FIN.6	Finland	Paula Karhu	6	Para 2.4	Modify: “…and the information security management system of a competent authority or regulated entity should reflect the information security measures and activities necessary to support the nuclear security and safety regime, as some functions (e.g. the safe operation of nuclear facilities) directly relevant to the State's nuclear security and safety objectives rely upon…”		X	Addressed with "…the nuclear security regime and it's interfaces with nuclear safety" which also aligns better with the example given.		
CAN.12	Canada		12	2.4	Define abbreviation ISMS for “Information Security Management System” and use throughout the document.	ISMS is a well-understood term from ISO 27001, and IEC 62645 uses cyber security management system (CSMS).This comment may increase clarity.	X	Uses of the term within the document do not meet the IAEA’s threshold for allowing abbreviations. A footnote was added on first use to indicate that ISO/IEC use of the abbreviated acronym.		
FIN.10	Finland	Paula Karhu	10	Para 2.4	Modify: “…should reflect the information security measures and activities necessary to support the nuclear security and safety regime, as some functions (e.g. the safe and secure operation of nuclear facilities) directly relevant to the State's nuclear security and safety objectives rely upon the confidentiality, integrity and availability of sensitive information”Text of Figure 1 should read “security and safety objectives”.	Same as in comment 1.	X			

USA.1	United States of America	Jeff Bream	1	Section 2, specifically a new 2.5	It would be useful to define “information” before 2.5. (e.g., “Information is…”). Consider using the definition in NSS 23-G paragraph 2.2.	“Sensitive information” is defined in 1.5 but “information” is not defined in the document. It is assumed that the reader knows the definition of “information” and what that distinction is (and how it is different than “information object” as discussed in 2.7). It may be useful to strengthen the connection between the three terms (information, information objects, information assets)	X			
OMN.2	Oman	Prof. Khalid ALNabhani	2	Page 7 Line 4-7 after the image Paragraph 2.5	We propose revising Paragraph 2.5 to state as follows: "An information object as “knowledge or data that have value to the organization” [2]. Information objects can be tangible physical or digital collections of information on paper, on film, on magnetic or optical media, in charts, in documents, in software executables, and in other forms and channels for transferring/transmitting information, *or information assets based on the individuals' knowledge, which are confidential information that is known to key persons within the nuclear facility, vendors, or regulators*”	This is due to the fact that: In the event that such sensitive information being disclosed or exchanged during informal discussions, under coercion, or through breaches of integrity—including knowledge assets related to nuclear material inventories, facility designs, safety system design networks, information systems, technical specifications, and other pertinent details as outlined in Paragraph 2.20—there exists a substantial risk that unauthorized dissemination or misuse of this information could expose vulnerabilities. Such vulnerabilities may be subject to exploitation in the context of criminal activities or deliberate unauthorized actions, thereby jeopardizing nuclear safety, national security, and nonproliferation initiatives.	X	Tangible and physical have been addressed in the document. The statement that information objects are information assets was not addressed as it is not consistent with the definition of information object and information assets established within Section 2 which are distinct concepts. Additionally, this also does not align with the definition of (Sensitive) Information Asset within the NS Glossary.		
TUR.1	Türkiye	NRA	1	2.6. (a)	(a) The information within an information object shares a common usage, purpose, associated risk, environments for creating and processing and form of storage or transmission	In addition of storage and transmission, the activities of processing or creating the information should be also taken into consideration.	X	Added with minor modifications to retain existing format and add "typically"		

CAN.13	Canada		13	2.7	Remove incorrect statement:“It is only when the information can be treated as an information object (i.e. is tangible, can be labelled and is in the appropriate context, can be viewed) that practical measures for information management can be used.”	Practical measures can be taken to protect intangible information. For instance, data inside a computer is intangible, but could be protected by protecting the computer itself.Knowledge is intangible but can be protected by screening people before allowing them to access the information, by compartmentalization and associated administrative procedures that manage clearance and need to know. Verbal communication can be protected by use of a secure compartmentalized information facility (SCIF).	X	Changed ‘practical’ to ‘targeted and specific’ also in 2.14.		
USA.6	United States of America	Jeff Bream	6	Section 2.12		This diagram is very helpful to the illustration of the definitions. Perhaps this diagram should be broken into sections as each definition is discussed. It will provide a visualization of the definition providing clarity as each element is introduced.	X	Subheadings corresponding to Figure 2 have been applied to the adjacent text, to provide strong alignment with Figure 2.		
FIN.11	Finland	Paula Karhu	11	Para 2.13	Delete: “It is difficult to apply targeted and effective information security measures to protect information in its abstract form, without context and without the labels to convey its value.” May be replaced by: “Hence information security measures should cover information as comprehensively as practicable in its tangible and abstract forms.” or similar.	Stating that something is difficult does not provide guidance. Instead, we should write what can and should be done. In the case of abstract information, such as ensuring confidentiality of certain knowledge, administrative measures, e.g. training on information security, should be applied, even if technical controls might not be effective.	X			
FIN.7	Finland	Paula Karhu	7	Para 2.14	Move vendors to be a separate item on the list, possibly a new (f) and modify “Third parties, such as supply chain, i.e. vendors”.	To emphasize the importance and universal character of this risk vector, which is relevant to government organizations and nuclear facilities alike.	X			
DEU.3	Germany	Germany/Technical University Munich, FRM II	3	2.18, last sentence	“If the calibration table is manipulated, multiple functions could be adversely affected, which means that both the sensor data, the	Clumsy wording in the phrase “… both the sensor data the calibration table, the calibration algorithm, and any associated set points should be assessed …” For grammatical reasons, some correction is necessary.	X			

					calibration table, the calibration algorithm, and any associated set points should be assessed as sensitive information.”					
FIN.8	Finland	Paula Karhu	8	Para 2.19 and similar sentences elsewhere	Add: “…loss of integrity or availability can also have negative consequences for nuclear security and safety.”	Same as in comment 1.2.19 is a prime example, as it addresses loss of availability or integrity, which are super important for example in accident management.	X			
FIN.9	Finland	Paula Karhu	9	Para 2.19	Consider adding: “Authenticity and non-repudiation could also be considered. Authenticity ensures that the information comes from a known source which is not impersonated by someone else. Non-repudiation ensures that the receiver or sender of information cannot deny sending or receiving or accessing information, minimizing the insider risk.”	For completeness.	X	Added as a footnote, the document has been authored considering that these are aspects of Integrity under a basic CIA triad.		
USA.2	United States of America	Jeff Bream	2	2.23 (and throughout where safety, securing, and NMAC are referenced)	Add emergency response to the list.	Is emergency response a concern as well? It is an example in I-6(f)(iii).	X	The norm in IAEA NS publications is to use "nuclear security and nuclear safety" to cover everything with EPR considered a constituent part of nuclear safety. Similarly NMAC is a part of nuclear security so instances of NMAC being called out explicitly were removed. Both have been clarified as being constituent parts in footnotes.		
FIN.13	Finland	Paula Karhu	13	Para 2.25 or 2.26	Add: “Users should be unequivocally identified and	For forensics reasons, for example. Also to avoid unintentional disclosure to persons without access.	X	Added without the term "unequivocally"		

					authenticated.””Lists should be maintained of persons who have access.”			in discussion with comment author.		
DEU.4	Germany	Germany/Technical University Munich, FRM II	4	2.27, 4th sentence	“Specific guidance on measures to protect against internal adversaries can be found in IAEA Nuclear Security Series No. 8-G (Rev. 1), …”	Insertion of a missing word.	X			
USA.9	United States of America	Jeff Bream	9	Section 2.28c	Replace the second sentence in this section with: The area referred to as “sensitive digital assets” in Figure 3 is where sensitive information assets intersect with computer-based systems. This area is the domain of computer security for nuclear security.	It is unclear what is meant when we introduce the term “domain” on the third line of this section. This seems to imply that “computer security” only refers to sensitive digital assets. Computer security is commonly thought of as the security of all computer-based assets. All nuclear facilities should proportionately apply the principles of computer security to all their digital systems, including those systems outside the scope of their State’s nuclear security regulations or the IAEA’s area of concern. I think we are trying to say, “computer security for nuclear security” is the domain that applies to “sensitive digital assets”.	X	Digital assets, within the diagram, is the scope of NSS 42-G rather than sensitive digital assets (which are a subset). So sensitive was removed from the suggested text.		
CAN.14	Canada		14	2.28 (a)	Delete reference to unauthorized individuals.	Not clear how information security be applied to “information held, processed and communicated by … unauthorized individuals”. When an unauthorized individual holds sensitive information the security of the information has already been compromised.	X	This was addressed through restructuring 2.29 and changing the title of the subsection for greater clarity.		
FIN.14	Finland	Paula Karhu	14	Para 2.28 (or somewhere)	Add: “Information and information assets should have an owner.”	Considered good practice, for example from risk management perspective (as risks, too, have owners).	X	Added as a new para/ approx. 6.18		
CAN.16	Canada		16	3.1 (c)	Recommend defining the term “information security policy framework” or rewording the text to “information security policies” and “information security framework”.It is recommended to also provide a figure that shows the relationships between information	“Information security policy framework” is a new concept introduced in this document and not used elsewhere in the NSS.	X			

					security policy framework, information security policy, information security framework and the ISMS.					
CAN.23	Canada		23	3.2	Recommend rewriting this sentence to be more clear, or if that is not possible, deleting it.“The State should provide for operators and other licensees requirements and guidance on the ways and methods of coordination, coincidence and adjustment of information security measures with physical protection systems (including transport), countering illicit trafficking and nuclear safety measures.”	1. This sentence is confusing. What is a “method of coincidence”. Why is the term, “ways and methods” used? Is there a difference between the words, “ways” and “methods”? Is this referring to “means and methods”?It is unclear how “transport” is a physical protection system.	X			
CAN.17	Canada		17	3.3	This section could be interpreted as being misleading. There could be entities that have access to sensitive information (i.e., have a need to know) that are not regulated entities (e.g., suppliers, or law enforcement).	“Regulated entities are those entities that have access to sensitive information within the nuclear security regime”	X	Clarified through the use of "may" and an additional paragraph at 3.11 about law enforcement activities.		

CAN.18	Canada		18	3.3	Clarify the statement: “*Alternatively, a State could create separate information security requirements for competent authorities to follow.*”	It is not clear what this means. Are these information security requirements applicable to the competent authority, or are these information security requirements that the competent authority is to apply to entities that it regulates?Private entities (e.g., operators / licensees) are likely to have different classification schemes for sensitive information than government entities (e.g., competent authorities). This paragraph should be rewritten to capture this significant difference.	X			
CAN.19	Canada		19	3.8	Remove the sentence: “*Laws enacted for this purpose should mandate sanctions or punishment for unauthorized disclosure, manipulation or falsification of sensitive information.*”	This is too broad and not a graded approach. e.g., does this apply to all classes of sensitive information (or just the highest classes), and for all offenses (or just severe offenses)?Further, sanctions could be specified in a regulation rather than a law.	X	Changed ‘mandate’ to ‘enable’.		
FIN.15	Finland	Paula Karhu	15	Para 3.8	Add: “unauthorized disclosure, storing, manipulation or falsification…”	Also storage in an inappropriate place may be a source of risk.	X			
CAN.20	Canada		20	3.9	Recommend that this be reworded to ensure alignment of information across the legislative framework.	This considers other laws as examples. This is connected to the previous comment (para 3.3) outlining that private organizations and government organizations will likely have different obligations under the law for the protection of information.	X			
DEU.5	Germany	Germany/Technical University Munich, FRM II	5	3.9, 1st sentence	“The State should consider examples from other laws and international legal instruments (e.g. conventions such as Refs [8, 9]) to assist in defining and implementing information security as it relates to nuclear security.”	This is the right place to add references to the Amendment to the Convention on the Physical Protection of Nuclear Material [8] and the International Convention for the Suppression of Acts of Nuclear Terrorism [9]). These international legal instruments are included in the reference list, but nowhere cited in the text of NST070.	X			
DEU.6	Germany	Germany/Technical University Munich, FRM II	6	3.11, 2nd sentence	“IAEA Nuclear Security Series No. 29-G, … provides more information on such responsibilities [10].”	Grammatical correction: ‘provides’ instead of ‘provide’.	X			

CAN.21	Canada		21	3.13	Move clause 3.13 to before clause 3.12.	Improve readability. This is because the coordinating mechanism/body introduced in 3.13 will affect the policy framework discussed in 3.12.	X			
CAN.11	Canada		11	General3.14 (and other locations in the document)	The term “regulated entities” and “regulated entity or competent authority” should be replaced with “relevant entities” to align with NSS 42-G.	When referring to multiple entities it is clearer to use a single term (“relevant entity” rather than listing them). This causes confusion e.g., para 6.42. “*A designated team within the regulated entity or competent authority should prepare an incident response plan*”. This could be interpreted to mean that the competent authority prepares the incident response plan used by a regulated entity (or vice versa). Whereas “*A designated team within the relevant entity should prepare an incident response plan*” is clearer.	X	The term regulated entities will be assumed to refer to what may have made this confusing "regulated entities and competent authorities" should have been read as "regulated entities and regulated competent authorities". A distinction between regulated entities and relevant entities is defined in Section 3. Regulated entities has been normalised after 3.9 where a hereafter this term will be used note has been included. Before 3.9 "regulated entities and regulated competent authorities" has been used.		
USA.7	United States of America	Jeff Bream	7	3.19	… such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities …	Facilities with radioactive material are mentioned as facilities of concern. Not sure that this is consistent throughout the document. Recommend that is reinforced.	X			
CAN.22	Canada		22	3.19	Recommend deleting “*Actions could be necessary on the part of the State that are outside the scope of information security (e.g. placing requirements on information generated within other domains or applying the disclosure*	It is not clear what this statement is referring to or how it could be used to inform the development of the nuclear security regime.	X			

					requirements of other domains on information security)." unless an example could be provided to clarify what this means.					
DEU.7	Germany	Germany/Technical University Munich, FRM II	7	3.19, 1st sentence	"The State should ensure efficient functioning and performance functioning/performance of interfaces between information security and other elements of a State's nuclear security regime, …"	Clarification. In IAEA Nuclear Security Series publications, we generally avoid using a slash to separate words, with the exception of 'and/or'. The reason is that it is often not clear for the reader how to correctly read a phrase in which two words are separated by a slash, i.e. whether the slash stands for 'and', 'or', or 'and/or'.	X			
DEU.8	Germany	Germany/Technical University Munich, FRM II	8	3.19, 1st sentence	"… the detection of and response to nuclear security events.."	Minor editorial correction: removal of a surplus punctuation mark at the end of the sentence.	X			
CAN.24	Canada		24	3.22	This should be worded to delete any references to "objects" and "assets", perhaps as "*The State's information security policy framework should define criteria necessary to identify the information that the State wishes to protect and should indicate how information is to be protected.*"	Since "objects" and "assets" are specific to IAEA NST070 and not universally used in information security, it is unlikely that the any state's information security policy will meet this requirement.	X			
CAN.25	Canada		25	Risk Management (3.25 and 3.26)	Recommend: aligning risk management of information security with computer security from other NSS publications.	This section is critical but incomplete, and is not connected with risk management elements within NSS 42-G and NSS 17-T.Without information security, computer security risks are significantly increased. Risks should be holistically managed (e.g., computer security, information security …)	X	Risk management is addressed later in the document, a risk management approach isn't specifically described as it would likely be too detailed for an implementing guide and similar content was removed during internal editing. Clarification for coordination has been provided in the		

								Risk Management sub-section.		
FIN.16	Finland	Paula Karhu	16	Para 3.26	Modify: “The competent authority for information security should also cooperate closely with the national security authorities, including with the nuclear regulatory authority in order to devise the national threat assessment or design basis threat.”	The regulator may be involved in the threat assessment process and in many countries is responsible for the DBT.	X	Addressed as “other competent authorities in the nuclear security regime and” under the basis it would include the NRA and all others.		
DEU.9	Germany	Germany/Technical University Munich, FRM II	9	3.28, 2nd sentence	“… the regulated entities and competent authorities’ information security policy and information security management system.”	Minor editorial correction: insertion of a missing apostrophe.	X			
USA.10	United States of America	Jeff Bream	10	4.1	4.1. Implementing information security systems and associated measures involves both resources and time. It is neither feasible nor desirable to ensure that all the information (with an emphasis on information objects and assets) at a regulated entity or competent authority is protected in the same manner.	In Chapter 2 (including Figure 2 and Section 2.7), we define “information” as “abstract and unstructured” and lacking in “clear context and meaning”. Section 2 implies that information security is often focused on protecting more tangible products -- information objects and assets**. How do we make the transition from the Section 2 depiction of “information” to the broader definition of “Information” used in Section 4 which includes information objects and assets?** For example, this issue persists in Section 4.2 when we talk about “which information… constitutes sensitive information”. As I proposed in an earlier comment, this problem goes away if in Section 2 we stop using the term “information” when referring to unstructured data, and instead refer to it as “unstructured information”.	X			
CAN.26	Canada		26	4.1	Should be “… implementing information security management systems …”.If this is not correct,	The word “management” is missing.	X			

					please define “information security system” and provide context within the ISMS.					
CAN.27	Canada		27	4.1	Risk informed approaches should be referred to here as the basis for recommending a graded approach	NSS 20-F recommends the use of risk informed approaches for allocation of resources (clause 3.9).Risk informed approaches should be referred to here as the basis for recommending a graded approach. This requires connection to the risk management discussion in clauses 3.25 and 3.26 of this document (NST070).	X			
CAN.28	Canada		28	4.1	Remove “nor desirable” “It is neither feasible nor desirable to ensure that all the information at a regulated entity or competent authority is protected in the same manner.”	Desirable is subjective (as is “feasibility” to a lesser extent). This might not be the case for facilities having only a small amount of sensitive information.This should be connected to risk tolerance / acceptance of the State and should be tied to risk management.	X			
CAN.29	Canada		29	4.2 (a) and (b)	“Impact” and “Consequence” are used in this clause, and both refer to an effect. It may be helpful to tie the impact of compromise to the consequences listed in NSS 20-F (clause 3.9 (d))	This clause describes using the “impact of compromise” as the basis of a graded approach whereas NSS 20-F para 3.9 talks about the “potential harmful consequences” as the basis.	X			
CAN.30	Canada		30	4.2 (b)	Delete 2nd occurrence of “of”.	The word “of” is repeated.	X			
CAN.31	Canada		31	4.2 (c)	Recommend rewording by removing (c) and clarifying that the impact assessment in (a) and (b) needs to take the usefulness of the information into consideration.	The impact assessment in clauses 4.2 (a) and 4.2 (b) must take into account the potential usefulness of the information to the adversary.	X			
DEU.10	Germany	Germany/Technical University Munich, FRM II	10	4.2, item (b)	“… an attack designed and executed to mislead human or machine based decision making;.”	Minor editorial correction: at the end of the text in item (b), replace full stop by semicolon.	X			
CAN.32	Canada		32	4.3	It is recommended to create a new clause for the last two sentences of para 4.3.	Starting at “Some information that is not considered …” represents a different thought from the previous sentence.	X			

FIN.17	Finland	Paula Karhu	17	Para 4.3 (or other appropriate place)	Consider adding: "The responsibility of who should classify the information may be specified in the national information security framework and/or in an organization's information security management system."	Relevant for information life-cycle and clarity of responsibilities.	X			
CAN.35	Canada		35	4.6 (h)	It is unclear why information objects and process information are identified as assets. It is recommended to clarify what is meant by "processing" an information asset.	The use of "asset" and "object" may introduce confusion to the reader. This challenge was also observed in other clauses of this document.	X			
CAN.36	Canada		36	4.6 (i)	Recommend providing an example to clarify.	It is not clear what is being prioritized for classification and protection– information objects or information assets.	X			
CAN.37	Canada		37	4.6 (j)	Provide guidance that a threat and risk assessment should be performed (and periodically updated) as part of the classification process.	This isn't really a consideration for the classification scheme, but rather a consideration for the information security management system.	X			
CAN.38	Canada		38	4.6 (k)	Provide clarification as to the scope of information that this clause would apply to.	This states that all information should be assumed to be of the highest classification until proven otherwise.This seems to be overly burdensome, given that only a small proportion of operator information will ultimately be found to be requiring the highest level of classification.	X			
CAN.39	Canada		39	4.7	Add consideration for Top Secret, or equivalent levels higher than Secret.	The licensee may hold a copy of Design Basis Threat or national threat assessment, which could be classified higher than Secret.	X			
CAN.40	Canada		40	4.9 (c)	Consider rewording this clause for clarity. A possibility may be "*Using technology to manage complex classifications is a possible solution that may reduce the reliance on the understanding of the person performing the classification*".	This clause references "another solution", yet no other solutions have been proposed. Further, it is the owner (i.e., custodian) /creator of the information who is in the best position to classify the information and it should be their responsibility to classify it not the user of the information.	X			

TUR.2	Türkiye	NRA	2	4.13	(a) Location of the classified information both physically and digitally(b) Inspection, audit and exercise reports related to the security and safety related topics	(a) Location information of sensitive information has also a critical value, this kind of information can give an idea to adversaries for reaching the sensitive information. So, this kind of information should not be available to everyone.(b) This kind of reports has details regarding the structure and vulnerabilities of the physical protection system and othersystems critical to Safety and security.	X	(a) Was added as a new item (e)Was not added, the basis for these items is already covered under (j) which states “Details of vulnerabilities or weaknesses that relate to the above topics;”		
CAN.41	Canada		41	4.13	Add something similar to (a) which lists “Details of computer security measures …”	The list does not specifically address sensitive information related to computer security measures. While it could be argued that “any other security measures” covers computer security measures, this is something that should be explicitly mentioned.	X			
CAN.42	Canada		42	4.13	Recommend adding “authentication details for sensitive private and public accounts”.	For example, an operator’s official social media account or system domain administrator credentials.	X	Added to (e)		
CAN.43	Canada		43	4.13	Consider adding an example related to the transport arrangements for nuclear or radioactive materials.	While (a) could be interpreted as applying to nuclear materials in transport, it would be recommended to explicitly mention it for clarity.In addition, clause 5.12 references information related to the transport of nuclear material.	X			
CAN.44	Canada		44	5 (General comment)	It is recommended that section 5 be rewritten using a lifecycle from ISO 27000 or NSS 23-G. It should be connected to NSS 20-F, 42-G and 17-T.It also should be connected to risk management section of this document (NSS070), contained above, which currently does not discuss risk management throughout the lifecycle.	This section of the document could be misinterpreted by readers, and is difficult to follow. It would also benefit strongly from using a lifecycle taken from an appropriate published reference.	X	Addressed per. CAN.45 for the basis for the four-stage lifecycle. Additional references have been included to highlight the relationship between risk management, the lifecycle, and the ISMS.		

CAN.45	Canada		45	5.1	Recommend transitioning to a commonly used information lifecycle such as that referred to in ISO 27001, Annex A, 8.1: creation, processing, storage, transmission, deletion, and destruction.	A rationale for this change is that the IAEA has a practical arrangement with IEC and the IEC standards are based on the ISO 27000 series.	X	The lifecycle presented in the document is an information lifecycle rather than an information/computer security lifecycle. There is no equivalent in in the ISO 2700X series. The generic lifecycle has been written as a number of stages that collect the various activities written into NSS 23-G as well as those that have been requested for address by other MS comments throughout both the development of the DPP and the comment process for NST070. This was previously addressed as a footnote but has been clarified within the document with a Figure added to ensure the relationships between the lifecycle stages is well understood. Additionally, an informative annex has been proposed aggregating the activites within NSS 23-G and the NIST glossary		

CAN.46	Canada		46	5.1	It is recommended to delete “archiving”. This term is not defined in the document, and the meaning of “archiving” an object is the preservation and storage of information for long-term retention and future access. That is to say, archiving is a form of storage. Furthermore, NST070 provides no specific recommendations for archiving, except for 5.27 where it is listed with storage. Stage 2 has “transmission of information” whereas stage 3 has “sharing … and dissemination of information”. It is not clear that these are sufficiently different (except perhaps as to degree - transmission à “to send forward to a recipient”, and dissemination à “to spread widely to multiple recipients”) to warrant identification in different lifecycle phases.	This is a novel lifecycle that has been changed from NSS 23-G which used “create, identify, classify, mark, handle, use, store, transmit, reclassify, reproduce, and destroy sensitive information”.Consider using the NSS 23-G lifecycle phases or consider using a more typical lifecycle, such as that identified in ISO 27000 series, as noted above or the NIST glossary (https://csrc.nist.gov/glossary/term/information_life_cycle “the stages through which information passes, typically characterized as “creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.”	X	Addressed archiving per disposition of CAN.53 and reference back in Section 6.		
CAN.47	Canada		47	5.1	Consider adding reclassification to the lifecycle.	Although 4.6 (j) and 5.24 notes that the need to classify information may change over time, reclassification has been removed as a lifecycle activity (it was present in NSS 23-G).	X			

OMN.3	Oman	Prof. Khalid ALNabhani	3	Page 23 Line 6-11 Paragraph 5.7	Paragraph 5.7 need to be revised to include also: " It is recommended to adopt quantum / post quantum resistant encryption—a form of encryption specifically designed to withstand attacks from quantum computers. This approach involves utilizing new cryptographic algorithms that do not rely on conventional mathematical principles, offering a higher level of security for sensitive data, such as that related to nuclear security. Implementing these advanced encryption methods will be critical to safeguarding against future threats posed by quantum technologies.	Given the swift advancements in technology and scientific fields, along with their increasing application in automating operational and security protocols within nuclear facilities, it is crucial to introduce recommendations that align with these developments, particularly in the areas of cybersecurity, Information Security, and Cloud Infrastructure Security. For instance, traditional encryption methods that are mostly based on mathematical algorithms are increasingly vulnerable to being broken by quantum / post quantum computing. As quantum computing embedded with artificial intelligence tools evolve, they possess the capability to process information exponentially faster than current systems, enabling them to decrypt even the most secure encryption algorithms in use today.	X	Addressed through the same footnote resolution in IND.2		
DEU.11	Germany	Germany/Technical University Munich, FRM II	11	5.8, 1st sentence	“The access of individuals to sensitive information should be controlled by a process or procedure that grants access on the basis of the ‘need to know’ principle and rescinds this access when this need no longer exists.”	Editorial correction: it is preferrable to insert the principle for dissemination of sensitive information in single quotation marks, in order to avoid an ambiguous statement as well as for internal consistency reasons – compare with the spelling in paras 2.25 (2nd sentence), 2.26 (1st sentence), and 4.11 (1st sentence).	X			
DEU.12	Germany	Germany/Technical University Munich, FRM II	12	5.8, 2nd sentence	“The ‘need to know’ principle could nevertheless be perceived as incompatible with the overall need to share information …”	For justification, see German comment No. 11.	X			
CAN.48	Canada		48	5.11	It is recommended to clarify that controlling physical copies of material is still applicable to protecting physical documents.	The document should provide guidance for protection of information based upon its form.Since information may be in physical form (e.g., a document, a USB drive, other media) physical protection is still required.	X			

CAN.49	Canada		49	5.12	It is recommended to clarify this clause.	This clause could be misinterpreted, and the purpose for this clause is unclear.	X			
CAN.50	Canada		50	5.13 and 5.14	These clauses should clarify what the distinction is between information sharing and information disclosure, so that the later clauses can be reviewed for appropriateness.	These clauses talk about “disclosure” and “sharing” and both disclosure and sharing are discussed later in section 5 as having differing requirements.It is not clear what the difference is between “sharing” and “disclosure” since both talk about transfer of information to other entities.	X			
CAN.51	Canada		51	5.22	Should clarify what the difference is between sharing and disclosure.	A clarification of the difference in these two terms will improve clarity of message.	X			
CAN.52	Canada		52	5.22	“…in deciding which sensitive information can be disclosed.”	The guidance developed by the State will depend on the audience for the disclosure. It is recommended to indicate that guidance may differ depending on the information’s audience.	X			
CAN.53	Canada		53	5.27/5.28	As mentioned in above recommendations for clause 5.1, archiving should be discussed in the section on storage. If there are no differences in the guidance for “storing” and “archiving” then discussion of “archiving” as a separate activity should be removed.For clarity, downgrading is recommended to be discussed with the clauses on classification (i.e., in section 4).	Destruction, downgrading and archiving are distinct activities with different requirements.Downgrading means reassessing information and determining that it should be classified at a lower level.Destruction makes the information no longer available for use.Archiving refers to long term storage of information that may be accessed later.	X	Clarification has been added to 5.28 and 5.29. Archiving is more focused on record retention than storage during use so remains in 5.x.		
IND.4	India	Dr. Garima Sharma	4	Page No. 26may be included as para 5.29	Align destruction and archival practices with international standards and best practices, such as those established by organizations like ISO. Specific ISO standards relevant to sensitive information destruction and archival include:ISO 27001: Information security management system (ISMS).ISO 27002: Code of practice	Destroying or Archiving Information	X	Reference was added to alignment with international standards and good practices.		

					for information security controls.					
CAN.54	Canada		54	6 (General comment)	Please clarify and define the various terms used in this section, such as “legislative and policy frameworks”, “information security management system”, “information security policy frameworks”, etc.	Generally, this document does not maintain consistency with the usage of some terms, and this may cause readers to interpret that the various sections are not well-connected to each other. The clarification of these terms should be in section 2 (“concepts”) and the paragraphs in section 6 should refer back to the concepts in section 2 (and to other sections)For example, footnote 7 should be in section 2.	X	The terms were clarified downwards from Section 2 to Section 6 and other sections. Footnote 7 was moved to the first use of ISMS and references to Section 3 as appropriate. Multiple reviewers could not ascertain the described inconsistency in terms.		
CAN.61	Canada		61	6.1	Remove “formally”.	Not clear the difference between “documented” and “formally documented”. The management system usually defines the requirements for documentation.	X	Attempted clarification with a list of examples rather than deleting		
DEU.13	Germany	Germany/Technical University Munich, FRM II	13	6.1, Footnote 7, 1st sentence	“The International Standard for Information Security, ISO-27000 ISO/IEC 27000 [14], uses the term ‘information security management system’.”	ISO/IEC 27000 is a dual logo international standard, jointly approved and published by both ISO and IEC. This standard needs to be added to the list of references (see also German comment No. 17).	X			
CAN.55	Canada		55	6.2	The text starting at “The policy should articulate high-level goals …” should move to section 2.	This is background and should be included in section 2 of this document (Concepts)			X	This is the first place where an ISMS in a facility is described in general. In Section 2 it is mentioned with further reference directed to Section 6.
CAN.67	Canada		67	6.2	Recommend a change to “… information security (including computer security) …” or equivalent.	Computer security (i.e., NSS 42-G) is missing from the text.	X			

CAN.68	Canada		68	6.2	Recommend including text to indicate that effective management should consider risk.	This clause discusses threats and meeting requirements, but does not discuss meeting risk thresholds.	X			
DEU.14	Germany	Germany/Technical University Munich, FRM II	14	6.2, 1st sentence	“Regulated entities and competent authorities within the sState’s nuclear security regime should develop …”	Editorial correction: initial capitalization of the noun ‘State’.	X			
FIN.18	Finland	Paula Karhu	18	Para 6.2	Add: “In an organization, the top management is accountable for information security.”	As a reminder and for awareness raising purposes.	X	Added as “senior management commitment and accountability”		
CAN.56	Canada		56	6.3 and 6.4	Clarify that the ISMS needs to require risk identification, analysis, and evaluation (i.e., risk assessment), that then provides recommendations on treatment of risks.	Goals, objectives, requirements and resources are all inter-related and must be risk informed.These are dependent upon risk management activities within the ISMS.	X	Added to 6.6 as earlier paragraphs are discussing the generalised concept of a management system.		
CAN.77	Canada		77	6.4	Recommend removal of the word “sudden”.	All incidents are “sudden” upon detection.Suggest that “Significant incidents… “ or “Severe incidents …” would be better.	X			
FIN.19	Finland	Paula Karhu	19	Para 6.4, line 5-7	Modify: “This Information security management system should be part of integrated with the integrated management system of the regulated entity or competent authority’s other management systems (e.g. together with safety, quality, physical security and computer security) in a coherent manner…”	To emphasize the concept of integrated management system, which is a good practice.	X	Proposal left a dangling reference to integrated management system so a rewording was attempted.		

OMN.7	Oman	Prof. Khalid ALNabhani	7	Page 32 Line 34-40 Paragraph 6.40	**Comment #** In the context of nuclear security requirements, and the fact that nuclear information security poses a substantial threat to the safety and security of nuclear operations, it is imperative to integrate this category of threats into the risk classification framework delineated in ***Table 1: Emergency Preparedness Categories in the IAEA Safety Standards for the Protection of Persons and the Environment — Preparedness and Response to a Nuclear or Radiological Emergency — General Safety Requirements No. GSR Part 7.*** Where, it is essential to develop a comprehensive guide detailing the procedures for the preparedness and response plan in addressing information security incidents, along with the specifications for the response team tasked with swiftly mitigating these threats prior to the occurrence of any potential disaster.				X	The document under review in Step 8 is NST070 which is a draft for the first revision of NSS 23-G. Step 9 of NST070 cannot integrate new content into GSR Part 7, however this material has been reviewed and developed based on comments from EPRESC and interfaces with all safety committees.
CAN.59	Canada		59	6.7 and 6.8	These clauses should identify how the objectives are determined and there is an absence of connection to risk management activities.	The assessed risks should inform the objectives (e.g., ISO 27001:2013 - information security objectives should take into account the applicable requirements and results arising from risk assessment). The ISMS manages the identified risks.	X	Added 'in a risk-informed approach'		

CAN.60	Canada		60	6.9	The risk management should identify the interdependencies with other programs and establish appropriate interfaces for coordinating activities needed by the ISMS and the interdependent program.	This text has been drafted in an overly prescriptive manner, which may be limiting.For example, the ISMS might interface with the corrective action program to address vulnerabilities and risks.	X	Original text was the basis of an IMS. Lowered from should now the IMS basis is elsewhere.		
CAN.62	Canada		62	6.12	This clause is repetitive from earlier sections of this document.	Resources are discussed earlier in the document and need to be risk informed.			X	Resources are only previously discussed for the competent authority for information security.
DEU.15	Germany	Germany/Technical University Munich, FRM II	15	6.14, 1st sentence	"A robust nuclear security culture (see IAEA Nuclear Security Series No. 7, Nuclear Security Culture [13]) is particularly important for information security in the nuclear sector because of the broader set of personal responsibilities involved."	This is the right place to add a reference to IAEA Nuclear Security Series No. 7 [13]. This publication is included in the reference list, but nowhere cited in the text of NST070.	X			
CAN.63	Canada		63	6.15	Recommend adding that the entity conduct an assessment or evaluation of the information security culture.	This clause is missing an evaluation or assessment element, as well as a feedback loop from the results of that evaluation or assessment element.	X			
CAN.64	Canada		64	6.18	Remove "formal".	It is not clear how "formal training" differs from other training that a person may receive, to achieve learning outcomes.	X			
CAN.65	Canada		65	6.19	Clarify that requirements are likely to be defined in policies, standards or guides.	The requirements are unlikely to be in procedures, and are more likely documented in higher-level management system documentation.	X			
CAN.66	Canada		66	6.19	Not clear to what "minimum encryption security lifetime" refers. "An example would be the minimum encryption security lifetime used for the electronic transmission of information."	It is recommend to clarify this phrase. Is the term"algorithm security lifetime" as per NIST SP 800-57 Rev 5 ("the estimated time period during which data protected by a specific cryptographic algorithm remains secure, given that the key has not been compromised.").	X			

CAN.69	Canada		69	6.21	Recommend moving this clause to section 2, concepts.	This clause is very high level, and perhaps could be better served in section 2 (Concepts).	X			
IND.1	India	Dr. Garima Sharma	1	Para: 6.22 (f)Page No. 29-30may be included	Leveraging Artificial Intelligence and Machine Learning for threat detection, anomaly detection, and automated response enhances security by rapidly identifying and mitigating potential threats with greater accuracy and speed. These technologies analyse vast amounts of data to spot irregular patterns and predict risks, thereby improving responsiveness. However, the deployment of Artificial Intelligence in nuclear security necessitates careful consideration of ethical and security implications. Issues such as algorithmic bias, decision transparency, and potential adversarial attacks must be addressed to ensure these systems are reliable and fair.	6.22. The following security measures should also be considered in the context of sensitive information:	X	Mentioning AI/ML may exceed the scope of the document as implementing guidance, the following paragraph is proposed to capture the detection/monitoring intent of the proposal: *(e) A system should be in place to identify, monitor and assess potential security incidents, encompassing both physical and digital threats to sensitive information, while enabling timely response to unauthorized access attempts, or anomalous activities that could compromise information confidentiality, integrity, or availability.*		
IND.2	India	Dr. Garima Sharma	2	Para: 6.22 (g)Page No. 29-30may be included	Quantum computing poses a significant threat to information security by potentially undermining current cryptographic systems, such as Rivest–Shamir–Adleman (RSA) and Elliptic curve cryptography (ECC), which rely on the difficulty of factoring large numbers or solving discrete logarithms. Quantum computers, leveraging		X	The suggestion doesn't fit in the list, which is about security measures. Added an example to (d) and the text as a footnote to 5.28 with slight rewording to reduce the length of the footnote: *Quantum computing might undermine current cryptographic systems, such as Rivest–Shamir–Adleman (RSA) and*		

					principles of quantum mechanics, could efficiently solve these problems, rendering conventional encryption methods vulnerable.			*Elliptic curve cryptography (ECC), which rely on the difficulty of factoring large numbers or solving discrete logarithms. Quantum computers could efficiently solve these problems, rendering conventional encryption methods vulnerable.*		
IND.3	India	Dr. Garima Sharma	3	Para: 6.22 (h)Page No. 29-30may be included	Securing IoT devices and networks in nuclear security is vital due to their integration into critical infrastructure, which increases vulnerability to cyber threats. These devices often have limited computational resources, making traditional security measures challenging to implement. To protect against potential attacks, a comprehensive security strategy must include strong authentication, encryption, and regular software updates. Additionally, network segmentation and anomaly detection can help mitigate risks by isolating and monitoring IoT devices for unusual activities. Addressing vulnerabilities involves securing communication channels, conducting thorough risk assessments, and adhering to best practices in IoT device management to ensure the resilience and				X	The proposed text is focused more on computer security than information security, NST070 has excluded specific guidance on computer security from its scope instead directing to NSS 42-G.The proposed text is relevant to NSS 42-G and could be considered in a future revision of that publication.

					integrity of nuclear security systems.					
CAN.70	Canada		70	6.23	Consider whether to keep this clause, as it is repetitive from earlier clauses.	The concept presented was previously discussed in clause 4.3.	X	While it appears repetitive 4.3 deals with classification and 6.23 deals with the decision of/application of security measures.For example measures resulting in workplace monitoring may not be permitted by privacy regulations but has no impact on the classification.		
CAN.71	Canada		71	6.24	Recommend to further clarify “third party”. Is this limited to suppliers, vendors and other parties to supply arrangements?	The use of “third-party” is not clear in this case.A third party could be a staff of a technical support organization accompanying an inspector from a competent authority to perform an inspection of a licensee’s ISMS. In this case, many of the clauses relating to third parties (e.g., those involving contractual arrangements) are not applicable. Therefore, the text of this clause may need to be amended.	X			

OMN.4	Oman	Prof. Khalid ALNabhani	4	Page 30 Line 24 "***Arrangements with third parties***"	Under the section titled 'Arrangements with Third Parties,' it is recommended to add an additional point as outlined below 6.28 **Approved Third Parties & Secured Nuclear Supply Chain** (a) Nuclear facilities shall exclusively procure equipment from suppliers accredited by the IAEA or pertinent international bodies to guarantee adherence to nuclear security standards, thereby mitigating cyber threats and enhancing operational safety. (b) Nuclear facilities are required to perform comprehensive technical inspections on all supplied equipment prior to deployment, ensuring the detection and mitigation of any vulnerabilities or malicious software. (c) All suppliers shall execute Confidentiality and Information Security Agreements, affirming their dedication to stringent data protection standards including a declaration of full legal liability, certifying that all supplied equipment have been tested, verified, and are free of vulnerabilities and malicious software. (d) Continuous audits shall be conducted by the nuclear facility to ensure ongoing compliance of suppliers	It is imperative to integrate a new clause within this section that acknowledges the indispensable role of the International Atomic Energy Agency (IAEA) and its experts in facilitating the enhancement of nuclear security among Member States. This clause should articulate the provision of technical counsel through the formulation of approved lists or processes for third-party entities engaged in nuclear supply chains to ensure their compliance with the stringent specifications and standards set forth by the IAEA .			X	These are not a structure or service the IAEA or other international organisations currently have in place and exceeds the authority of an implementing guide in the nuclear security series by mandating "shall" statements.

					and their equipment with established security protocols, including the management of software updates and the identification of emerging threats, in alignment with IAEA guidelines.					
OMN.5	Oman	Prof. Khalid ALNabhani	5	Page 31 Line 19 " ***Information security management system activities for insider threat mitigation***"	**Comment #** This section needs to be revised to include additional information related to 'Social Engineering' for the reasons provided here	Social engineering' represents a substantial threat to personnel within nuclear facilities, as adversaries exploit human vulnerabilities to manipulate individuals—who may unwittingly become insiders—into divulging sensitive information or compromising established security protocols. Despite the gravity of this issue, it has not been sufficiently addressed in this guideline or referenced other related and existing guidelines. Consequently, it is crucial to refer ti this issue here and to underscore the necessity of instituting rigorous protocols for the handling of sensitive information, along with the implementation of comprehensive training programs for personnel to enhance their ability to identify and counter social engineering tactics. Such measures will significantly bolster security awareness and mitigate the risks associated with these insidious attacks.	X			

CAN.72	Canada		72	6.33	Consider editing, “metrics” to “metrics or criteria”	Metrics may be too limiting particularly if quantitative measures are infeasible.	X			
CAN.73	Canada		73	6.35	“**internal** inspections”	Considering adding clarity that a relevant entity would do a self assessment or hire an independent auditor to assess its own programs.However, competent authorities would conduct inspections (as per 6.36) of regulated entities as a compliance verification activity. This would not be an “internal inspection”.	X			
CAN.74	Canada		74	6.37	Recommend rewording to clarify that inspections do not recommend corrective actions. Need to clarify who develops the corrective actions.	Inspections by a competent authorities identify deficiencies (e.g., non-compliances/violations) that need to be corrected, however, they do not recommend corrective actions. It is up to the regulated entity to develop the corrective actions which would be accepted by the competent authority.	X	Accepted the comment that inspections do not directly recommend corrective actions. However modified to read that it can be either the regulated entity or the competent authority for information security that does identify the corrective action to allow for different approaches in different States depending on the particular approach to regulation.		
CAN.75	Canada		75	Section starting at 6.39	This is not well aligned with NSS 17-T (and IAEA TDL-005)	Recommend ensuring consistency with NSS 17-T Rev 1.	X	Both NSS 17-T Rev. 1 and TDL-005 are specific to both computer security and nuclear facilities whereas NST070 is cross-cutting and applicable to the broader domain of information security. A reference was added as 6.41 and relevant terms (e.g. incident response plan) were confirmed to be consistent. TDL-005 is also outside of the NSS so		

								NSS 17-T Rev. 1 is the sole reference point.		
CAN.76	Canada		76	6.39	Recommend that text be reworded as follows, “These incidents can range from unauthorized disclosure of sensitive information to alteration or manipulation of sensitive information that causes a nuclear security impact (see figure 5)”.	The current wording is confusing and could be misinterpreted.For instance, a change in information initiates maloperation of a system resulting in sabotage.	X			
OMN.6	Oman	Prof. Khalid ALNabhani	6	Page 32 Line 27 "***Detection of and response to information security incidents***"	It is imperative to incorporate the following under this section: Zero-day exploits pose a significant threat to information security in the realm of nuclear safety, as malicious actors may leverage unknown vulnerabilities within critical operational and security systems, including Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and Instrumented Safety and Control Systems (ISCS). The potential compromise of sensitive nuclear operations and data underscores the urgent need to fortify nuclear information security through the implementation of				X	The proposed addition of zero day exploits is focused on computer security. Per 1.9 this is the domain of protecting sensitive digital assets, the comment is addressed through the computer security strategy strucutre proposed in the published version of NSS 42-G. Further information in NSS 23-G or the introduction of new terms would be redundant.

					proactive cybersecurity strategies. These strategies should encompass comprehensive penetration testing, robust bug bounty programs, and other innovative initiatives. Such measures not only directly address zero-day vulnerabilities but also integrate into the overarching framework of nuclear information security, effectively safeguarding against sophisticated cyber threats that could jeopardize the operational safety, security, and integrity of nuclear facilities.					
FIN.20	Finland	Paula Karhu	20	6.42 (e)	Add: “Any risks in relation to nuclear security and safety within the State should be appropriately communicated to the relevant parties.”	Same as comment 1.	X			
FIN.21	Finland	Paula Karhu	21	6.42 (g)	Add: “Outline methods to recover information assets and information…”	Information systems may also need recovery, such as removing malware or adversary remote access, or reloading software, to re-establish a safe process.	X			
CAN.78	Canada		78	6.45	The meaning of “… the chronology should be restored …” is unclear. Clarification is needed.	Does this mean that the chronology (i.e., timeline of the incident) should be recreated?	X			
CAN.79	Canada		79	6.46	The text of this clause could perhaps be better described in terms of a coordinating mechanism?	The text recommends that a “competent authority” reports to the “competent authorities” and could be misinterpreted or confusing.	X			

CAN.80	Canada		80	6.47	Recommend explicit reference to the head of the relevant entity.	There are often staff or people in regulatory affairs departments, government relations departments, regulatory program divisions, etc., at the regulated entities that would make these arrangements, and the original text may be limiting.	X	Wording has been added and an attempt to remove potential ambiguities within the proposed text and reason provided within the comment.		
FIN.12	Finland	Paula Karhu	12	Para 2.20 (b)	Consider adding: "…, including some details of the arrangements in information security regarding capabilities to detect and respond to incidents."	While some capabilities (such as forensics) may function as a deterrence, (which could also be added, if considered valuable), detailed information on some controls may aid the adversary to bypass them.	X	Added as a list of examples to existing clause (b), modification confirmed with the comment author.		
SWE.1	Sweden	Swedish Radiation Safety Authority	1	Figure 1 and associated text as appropriate	Use a different approach to highlight the governance structures than the redundant arrows on the right.	Proposed modification to enhance clarity.	X			
CAN.7	Canada		7	Figure 1	Recommend replacing "ensuring *Sensitive Information* in the State … " with "establishment of monitoring and review of …"	This is a risk management process that should align with ISO 27005 given its references to ISMS. Ensuring can only be performed after an ISMS is established.	X	Changed 'ensuring' to 'securing'. The diagram already represents		
CAN.8	Canada		8	Figure 1	"correct performance" is not defined in the document. Recommend changing to "performance"	It is also conceivable that complete/correct performance is not achievable.	X	Rather than removing changed to "satisfactory" to provide less absolutism than correct.Also addresses CAN.9		
CAN.9	Canada		9	Figure 1	"preserving …"	CIA properties and functions do not align well. CIA properties are not independent of one another. For example, modification of cipher text (integrity impact) is likely to result in the destruction (or rendering unusable) of the information (availability impact).	X			

USA.8	United States of America	Jeff Bream	8	Figure 2, Section 2.7, and throughout the document		This document has two definitions for “information”. There is (1) definition/depiction of “information” as unstructured information and the (2) definition of information that encompasses unstructured information, information objects, and information assets. These two very different definitions are confusing. I think we should use the term “unstructured information” when we refer to information that lacks context or meaning and reserve the term “information” for the broader categorization that includes information objects and assets.	X	Using “abstract” instead of “unstructured” as the draft already used the term.		
CAN.15	Canada		15	Figure 2	This figure introduces a concept of “organizational functions” which is not referred to in the text of the document.	The concept of organizational function should be explained and clarified in the document, particularly the relationship between “organizational functions” and the various types of functions (e.g., “functions”, “security functions”, “functions relevant to nuclear security”, “physical protection functions”) referred to throughout this document.	X			
USA.3	United States of America	Jeff Bream	3	Fig 4 6.24-6.27	Potentially add Technical Authorities to the figure or clarify in the CA or Third Parties text that they are considered in the realm of that group	Should Technical Authorities (e.g., Cyber Emergency Response Team (CERT), Cyber Security Incident Response Team (CSIRT)) be included in this figure and described in the section? They aren’t quite goods and services providers in the normal definition as a supplier and they may not necessarily be governmental entities, but they could be granted access to sensitive information. Also, is it necessary to include TAs in other sections (e.g., 6.24)?	X	The diagram has been modified to clarify that third parties hold vs. process sensitive information, e.g. CERTS. An example has been added in the text under the diagram.		
CAN.33	Canada		33	Figure 5	Recommend a change to the arrow from “least sensitive” to “most sensitive”; it should be unidirectional.	The arrow for “classification of information” is bidirectional, unlike all the other arrows in the drawing which point from “low” to “high	X			

CAN.34	Canada		34	Figure 5	This figure should be consistent with NSS 42-G. "no impact" does not align with NSS 42-G.	In 42-G "no impact" has requirements (i.e., baseline requirements which apply to everything). This should also be the case for non-sensitive information. For example, an approved procedure that is not sensitive to the nuclear security regime would require an independent reviewer and approver for any change to that procedure to protect the integrity (accurate and complete) of the information in the procedure. This is an example of a baseline requirement that would apply to non-sensitive information.	X	"No impact" has been added with the intent of applicability to organizations which may not solely participate in activities utilizing nuclear or other radioactive materials, for instance a medical clinic that operates a blood irradiator. In this regard there is no basis for mandating baseline requirements for all information held by the organization. The example provided would likely exceed the scope of a nuclear security regime. The diagram has been modified to show "Information Security Requirements for Sensitive Information" as the bounding of the bottom box to allow non-nuclear security specific requirements to not be precluded.		
CAN.57	Canada		57	Fig 6	Text in the diamond, "Effectiveness for achieving objectives"	The clarity of this text could be improved for increased readability and understanding. Does this mean "evaluation of effectiveness"?	X			
CAN.58	Canada		58	Fig 6	Recommend developing a figure based upon IEC 62645 Figure 1 or similar for consistency with other published standards.	This figure shows the "computer security programme" from NSS 42-G with a new label ("Information Security Management System").This may not be an accurate or model representation of an ISMS.	X	Adapted PDCA from the programme level cycle in Fig. 1 of 62645		

FIN.1	Finland	Paula Karhu	1	General	Question about scope	This would be another excellent candidate for a joint publication in security and safety series. We do not have information security for security only, it is by de-fault for security and safety. There is one information security framework, not separate for each S. The one and the same information security management system (ISMS) in an organization serves and is essential for both S's, as it also ensures integrity and availability of information in addition to confidentiality.			X	This is a revision of an existing implementing guide that is being developed following the approved DPP, and the draft is at Step 9. To develop a joint publication would mean to stop all work and go back to the DPP. The document does address this in 1.6 and in the body content which has been expanded with specific examples while sticking to the DPP scope to highlight coverage of nuclear security protecting nuclear safety functions from malicious acts, not just nuclear security being synonymous with physical protection. Future revisions may be considered for a joint publication addressing further .

ENISS.1	ENISS	C. Martin	1	General Comment	Type of sensitive information considered:The document is supposed to deal only with information that is sensitive to nuclear safety. However, in the text, sensitive information related to nuclear safety is also mentioned.For example, in 1.7, 2.3, 2.4, 2.18, 2.19 c), 2.32, 4.2 c), 4.3, 4.8, 4.13 d)Criteria taken into account to classify sensitive information:The regulatory framework of States should regulate only sensitive information related to nuclear safety and whose loss of confidentiality could have consequences for the interests of the Nation.However, NST070 recommends a broader coverage for regulation by considering not only the risk of dissemination of sensitive information but also the risks of loss of integrity and availability of this information. In France, the regulations in force (IGI1300) only relate to the sensitivity of information in the sense of confidentiality (risk to the interests of the Nation in the event of dissemination of information) and not in the event of its unavailability or loss of integrity.The paper recommends				X	The scope of the original publication of NSS 23-G included addressing integrity and availability (1.6, 2.10, 2.11, etc.), notes applicability of the information security definition to safety (4.2), and provides the same or similar examples for Safety in Annex II.The DPP for NST070 has been approved with a noted expansion of the guidance addressing all three aspects of information security as well as continuing with addressing all domains relevant to nuclear security. This comment is rejected under the basis of the Step 9 instructions to ensure MS comments are given precedence to observer comments with reference to FIN.4, FIN.6, FIN.8, FIN.20, FIN.1, FIN.3 among others.

					establishing a regulatory framework to maintain the confidentiality, integrity, and availability of sensitive information.For example, 1.11(a), 2.2, 2.4, 3.6, 3.10, 4.2(a)(b), 5.15, 4.9(a)(b)(c)The examples given in Annex II confirm that technical information related to nuclear safety is indeed considered as well as risks other than those related to confidentiality.					
CAN.1	Canada		1	General	It is recommended to consider restructuring the document.	Clarity of document would be improved by introducing the concepts in section 2, and then reinforcing them throughout the document (i.e., within the appropriate sections).For example, the following concepts should be introduced in section 2: lifecycles, risk management, information security management system (ISMS).	X			

CAN.2	Canada		2	General	The document should include recommendations for a security analysis methodology (i.e., provide guidance on how to perform the security functional analysis that underpins NST070).	The draft NST070 attempts to apply the functional approach used in NSS 42-G and NSS 17-T Rev 1 to the information protection domain. In the safety system domain, there is a rich history of functional analysis, over many decades, and extending the analysis to include security aspects of safety systems is a manageable task. Very limited work has been done in the realm of security function analysis. Terms like “deter, delay, detect” are often used in the generic sense and can be thought of as functions, but are rarely (if ever) form part of a systematic functional analysis. For example, time values may be assigned to delay for a security system, but not to particular information. Even with systems, little work has been done on the relative importance of each system or piece of information to nuclear safety, or to each other for that matter.This ‘security functional analysis’ appears to underpin NST070, so the document should provide guidance for a security analysis methodology (i.e., give advice to states on the how to perform this novel activity).	X	This same issue exists with 42-G and 17-T Rev. 1. A complementary technical guidance document (or TECDOC if provided as an example only) that underpins all of the aforementioned could solve the problem with more portable guidance. In this specific instance providing a detailed technical methodology would go beyond the scope of an implementing guide and the approved scope of this publication, requiring a revision of the DPP. It is well acknowledged however and an attempt has been made throughout the text to highlight where existing methodologies can be used in both the analysis of functions and the associated value/consequence.		

DEU.16	Germany	Germany/Technical University Munich, FRM II	16	List of references, Refs [8], [9] and [13]	Either insert references [8], [9] and [13] at suitable places in the text (case 1), or remove them from the list of references (case 2). In case 2, renumbering of references after Ref. [7] is necessary.	The Amendment to the Convention on the Physical Protection of Nuclear Material (Ref. [8]), the International Convention for the Suppression of Acts of Nuclear Terrorism (Ref. [9]), and IAEA Nuclear Security Series No. 7 (Ref. [13]) are nowhere cited in the main text of NST070. A reference list should include only those references cited in the text – see IAEA Style Manual for Publications and Documents in English, 2005 Edition, Chapter 11: Bibliographical references, Part II: Citation of references in the text, Paragraph 8 (page 52 in the manual). With regard to proposals for insertion of these references into the text, see German comments No. 5 and 15.	X			
DEU.17	Germany	Germany/Technical University Munich, FRM II	17	List of references, additional Ref. [14]	"INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018)."	ISO/IEC 27000 is referred to in Footnote 7 to para. 6.1 (see German comment No. 13). This dual logo international standard needs to be added to the list of references. Regarding the correct citation format, see Ref. [11] in IAEA Nuclear Security Series No. 17-T (Rev. 1).	X			

OMN.1	Oman	Prof. Khalid ALNabhani	1	Page 5 Line 10 ***"Objective"***	**Comment #** Overall, this guide proficiently identifies potential information security risks relevant to nuclear security in a broad context, many of which stem from information leaks by individuals and inherently sophisticated cyber-attacks. However, it lacks in providing robust and sophisticated technical strategies or actionable recommendations to effectively address these risks and mitigate their potential impact. As this document aims to serve as a framework for information security with the overarching goal of enhancing nuclear security, it is imperative to incorporate targeted recommendations for risk mitigation. For instance, the implementation of behavior-based threat detection approaches /systems, in conjunction with secure artificial intelligence tools, including machine learning and deep learning algorithms, can significantly augment monitoring capabilities for complex threats. By offering explicit guidance on mitigation strategies, this guide would not only enhance the efficacy of security measures but also reinforce the resilience of nuclear information				X	Resolving the comment would exceed the scope of an implementing guide in the nuclear security series. These concepts could be covered in separate or subordinate technical guidance or a TECDOC.

					systems and facilities against emerging threats					
TUR.4	Türkiye	NRA	4	I-4		For the awareness training the incident response plan steps for the information security incidents part and scenarios shouldbe also covered and included in the awareness training.	X			
TUR.3	Türkiye	NRA	3	I-6 (b)	(v) Existing vulnerabilities of the security systems and computer-based systems which are not eliminated yet and are documented after audits, inspections, exercises etc.	This information can also be used by the adversaries for their act of theft or sabotage by exploiting the vulnerabilities	X			
TUR.5	Türkiye	NRA	5	I-8		For testing security knowledge and awareness of the personnel, the phishing and other social engineering tests can be added because it is different than regular and periodic tests, it should be non-periodic that the personnel would notexpect it will happen at any exact time.	X	Noted that these should be added, they are already covered in Annex III I-6(c).		

FIN.22	Finland	Paula Karhu	22	Annex II	The division according to the CIA principles in the sensitivity column should be further re-checked and/or explained to ensure added value. Examples: 1.1. B – also availability applies, 1.6 A – also integrity, 1.8 – also confidentiality, 2.3 – also integrity, 4.3 – also availability, 5.2 B – also availability?At least an attempt could be made to list the most important attribute(s), in order of priority/importance? Additionally, perhaps a footnote could be added to remind that availability of all sensitive information is important to someone or in some context and that integrity of most information is important, for decision making.	In step 7 similar comment was rejected, based on Member States having expressed that the annex was very much needed. If that is the case, we should take extra care that it is not misleading and that it would serve those MS well.	X	A footnote is added to II-3. However the additional attributes have not been reflected as it is not intended as an exhaustive list and has been provided as an example only. The annex was reviewed in a CM with a group of multidisciplinary internataionl experts and suggested modifications have been included.		
DEU.18	Germany	Germany/Technical University Munich, FRM II	18	Annex II, Table II–1	Category “9. CONTINGENCY PLANS, RESPONSE PLANS AND EXERCISES”, subcategory 9.2, column “Rationale for sensitivity”, 2nd sentence: “Secure and reliable Secure/reliable communications would contribute to preventing this [II-4].”	Clarification. In IAEA Nuclear Security Series publications, we generally avoid using a slash to separate words, with the exception of ‘and/or’. The reason is that it is often not clear for the reader how to correctly read a phrase in which two words are separated by a slash, i.e. whether the slash stands for ‘and’, ‘or’, or ‘and/or’.	X			
DEU.19	Germany	Germany/Technical University Munich, FRM II	19	Annex II, list of references, Ref. [II–4]	“INTERNATIONAL ATOMIC ENERGY AGENCY, Method for Developing Arrangements for Response to a Nuclear or Radiological	These are the correct citation details for the Emergency Preparedness and Response Series EPR-METHOD 2003, to be used in IAEA publications.			x	Citation details are accurate per IAEA publications website

					Emergency, Emergency Preparedness and Response Series EPR-METHOD 2003, IAEA, Vienna (2003).”					
USA.4	United States of America	Jeff Bream	4	Table II-1	If this document is intended to cover both IT and OT information assets, there needs to be at least one example of an OT process system, similar to 1.6A.Also, 4.2 indicates IT systems (IDS, etc)… is this also for OT systems or is another example necessary?	If OT assets are covered in this document there should be additional examples.	X	The existing example 4.3 covers this desired scope, addressed through the removal of “IT”.		
DEU.20	Germany	Germany/Technical University Munich, FRM II	20	Annex III, I–1 to I–9	Correction of paragraph numbers in Annex III: III–1 to III–9 instead of I–1 to I–9.	Erroneous numbering of paragraphs in Annex III.	X	The multi-level lists were reset with the section break for landscape in Annex II. This will be fixed prior to publication.		
USA.5	United States of America	Jeff Bream	5	Annex III, I-4(p)	Separate into two topics.	Aggregation of data leading to change in classification level is one concept. Evolution of vulnerabilities and attack methods is a second concept.	X			