NST070, Information Security for Nuclear Security

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Australia	Vanessa Robertson	1	1.6	1.6. Groups or individuals wishing to commit a criminal or other intentional unauthorized act involving nuclear material or other radioactive material or associated …	We propose reverting some of the text back to the original (deleted) text. A criminal act is an intentional unauthorised act. The text should just not refer to criminal act because not every act would be considered “criminal” under all jurisdiction’s legislation. The other suggestion is to change “… nuclear and other radioactive…” to “nuclear or other radioactive …”. The criminal/unauthorised act may only involve nuclear or radiological. If “and” is used, then an act involving only one of “nuclear or radiological” would not necessarily be captured by the guidance.	X	"Nuclear or other radioactive" is accepted and applied. The changes to the wording for criminal or intentional unauthorised act was not actioned per the explanation to AUS.5.		
NSGC	United States of America	NRC	1	Section 1.7	Replace “[8]” with “Ref. [8]”.	The proposed revision is consistent with the format followed for citing references throughout the rest of the document. This comment also applies to other instances in Section 1 (Introduction) where an inconsistent approach is used for citing references.	X	The document has been reviewed and sanity checked, correct referencing was updated in e.g. 1.8 and footnotes 3, 4, and 5. The correct referencing style is 'Document Name [Reference Number]' in first usage and 'Ref. [Reference Number]' in subsequent usages. The comment was Accept/mod as it requested modifications to first usages for consistency. Consistency was achieved, just by normalising subsequent usages instead.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Russian Federation	Rosatom	8	1.8	Delete the link to the Safety-Security Glossary. Use the approach from the current edition of NSS 23-G with a separate glossary for this publication	The joint Glossary is not a publication from the NSS Series, it was not approved by the NSGC. The Glossary is based on terms from NSS publications, and not vice versa	X	The reference to definitions in the external Safety-Security Glossary, for "sensitive information" and "information objects" have been removed. A number of terms in the current revision of NSS 23-G's glossary were defined for explanatory purposes. These (compromise, function, least privilege, need to know, confidentiality, integrity, and availability) are now addressed as explanatory footnotes at their first relevant use. This is consistent with how confidentiality, integrity, and availability have already been treated within the current draft. Definitions are not provided for terms defined in higher level publications (i.e. competent authority, nuclear material, other radioactive material, radioactive material, sensitive information, and sensitive information assets). "Information security" is planned to be defined in the revisions of NSS 20/13/14/15, so no definition has been provided within NST070 to facilitate future consistency. Due to the small number of remaining terms (i.e. information object, information security management system, information security policy framework, and regulated entities), it is proposed that they are incorporated as in-text definitions, consistent with the approach for RUS.6. Therefore the comment is accepted with modification. Rather than creating a separate glossary, in each instance the relevant introductory text for a term has been modified to appear as an in-text definition.		
NSGC	Australia	Vanessa Robertson	2	Footnote 1 on page 6	… information technology (IT), operational technology (OT), …".	Operational Technology should also have it's acronym, OT, listed for ease of use of the guide.	X			
NSGC	Russian Federation	Rosatom	9	1.11	Use only one term "information security management system" in the NST070, move the footnote from para 6.1 on the difference between the terms "system" and "programme"	The term "programme" is used twice – in paragraph 1.11 and in a footnote to paragraph 6.1. In the rest of the NST070, the term "system" is used	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Australia	Vanessa Robertson	3	1.16	… transport of nuclear or other radioactive material …".	The use of "and" in this context means that transporting companies that only transport nuclear or other radiological material (but not both) would not be considered an intended audience for the publication.	X			
NSGC	United Arab Emirates	FANR	1	2.3	Suggest adding examples of how or which the adversary actions can affect the confidentiality, integrity, and availability of sensitive information, and how this failure is visible.	To clearly understand which actions can lead to these consequences.	X	Annex II already provides a detailed list of examples of why information is sensitive relative to the potential consequences of a compromise of C/I/A. Rather than introduce to the body text para. 2.22 has been updated to highlight potential consequences are covered in the Annex II examples. The visibility of failure can be extrapolated from footnotes 4-6. Further elaboration on how to detect failure in the body text would likely go beyond the scope of an implementing guide.		
NSGC	Japan	NRA	1	p.8, Para. 2.4, Line 7	Suggest removing footnote 8 and 9.	It is not clear why "nuclear material accountancy and control" for nuclear security needs to be singled out in this sentence, same as "emergency preparedness and response" for nuclear safety in the same sentence. Since these footnotes could send a misleading message, we suggest removing these two footnotes: 8 and 9.			X	While the intent of this is well noted the footnotes have been established to address requests from other MS comments to: i) Note the explicit inclusion of EPR/NMAC; and ii) Not distinguish EPR from Safety and NMAC from Security. Under this basis it is proposed that the two footnotes persist, as they resolve confusion for other MS.
NSGC	Egypt	Prof. Wael EL Gammal	1	2.8	The distinction between 'information' and 'information objects' is important because it might be difficult or less cost effective to manage information in a form in which it lacks clear context and meaning. Figure X provides a visual representation showing how abstract information is transformed into tangible information objects, which can then be properly classified, labeled and protected. This visualization helps security personnel understand when information transitions from abstract concepts to protectable objects	A visual diagram would clarify the sometimes-abstract concept of "information objects" versus raw information. This enhances the document's practical utility by helping personnel identify when information becomes a security-relevant object. The diagram would serve as a training aid and improve consistent application of security controls.	X	The visual diagram has been provided in FIG. 2.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					requiring specific security controls.					
NSGC	Egypt	Prof. Wael EL Gammal	2	2.15	When the information contained in information objects and information assets contributes to the performance of nuclear security related functions, a different value might be attributed to these objects and assets by each of the entities and organizations listed below: ... (f) Third parties and entities in the supply chain (e.g. vendors, contractors, suppliers, IT service providers, cloud computing providers). Supply chain risks like IT vendors and cloud providers deserve special attention as they frequently handle sensitive information while operating outside direct facility control. Their access privileges and protection measures should be explicitly addressed in information security plans with appropriate contractual security requirements.	Modern nuclear facilities increasingly rely on IT service providers, cloud computing, and external vendors who may process sensitive information. These entities represent a significant and growing attack vector that was not fully addressed in the original text. Explicitly mentioning these stakeholders emphasizes the need for comprehensive supply chain security measures.	X	This is addressed extensively in Section 6. An additional reference/example has been added to 3.9, which is referenced as the source of Section 6. Regulated entities would cover organisations with direct access.		
NSGC	Australia	Vanessa Robertson	4	2.21	(i) Details of the Design Basis Threat (DBT), Threat and Vulnerability Assessments.	The DBT, Threat and Vulnerability Assessments, as the basis for security planning/security measures, would be valuable information for an adversary.	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Australia	Vanessa Robertson	5	2.23	… "plan or commit criminal or other intentional unauthorised acts."	As mentioned in point 1, a criminal acts an intentional unauthorised act. So "other" either needs to be included to capture all intentional unauthorised acts, whether they are deemed criminal or otherwise. Once a formulation of words is determined, it will be important to check that the same formulation is used throughout the document.			X	The inclusion of "other" is currently being discussed within the development of NST072 the first revision of NSS 20.The proposal for NST070 is to use the term as currently published within NSS 20 as approved by the BoG, which is consistent with the current working direction in the NST072 development CM.If the terminology in the development of NST072 advances then this may also be reflected in the publication of NST070 later by the secretariat.
NSGC	United States of America	NRC	2	2.24	Change "plan" to "execute"	This activity seems more in support of executing rather than planning an attack.	X			
NSGC	United States of America	NRC	3	2.26	Suggested text. "Access to sensitive information, sensitive information objects, and sensitive information assets should be limited to individuals who genuinely need it to perform their job duties. Similarly, the sharing of sensitive information should be restricted to authorized personnel and resources, based strictly on a 'need-to-know' basis."	The first sentence groups sensitive information, sensitive information objects and sensitive information assets, regarding access by individuals. The second sentence then talks about dissemination of sensitive information to individuals and sensitive information assets. The different mixing of the terms here is confusing to read. I understand the differences due to access vs disseminate and what the intent of the paragraph is. However, it seems it could be simplified somewhat.	X			
NSGC	United States of America	NRC	4	2.27	Second sentence: This is because the risks associated with information security are more enhanced when sensitive information is shared by individuals who do not understand the potential value of the information.	Suggest adding red text to clarify the tie into the first sentence. Otherwise, it can be read to simplistically say people who do not know the potential value of the information may have the information – but just at a greater risk. This ties into the concept of graded or tiered levels of sensitivity which is discussed elsewhere.	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	United States of America	NRC	5	Section 2.29(b)	Revise this subsection to read as follows: "Security of sensitive information assets (e.g. information storage and processing equipment). Guidance on computer security for nuclear security can be found in Ref. [6] and Ref. [8]."	Despite the revisions made to Figure 3 (Relationship between the information and computer based systems in the State and in the nuclear security regime) and the associated text in this section in response to comments from Member States, its content is still confusing. For example: It is difficult to discern from Figure 3 the difference between "Sensitive digital assets" and "Digital Assets." Examples of "Sensitive digital assets" are referred to in Figure 3 as "Personal computers, programmable logic controllers (PLCs), servers, modems, sensors, software, and secure communication systems." While examples are not provided for "Digital Assets," Figure 3 depicts them as an intersection point between "Sensitive digital assets" and "Computer based systems." Related to the above comment, the "Digital Assets" depiction in Figure 3 unintentionally segregates the concept of computer security for the rest of the elements in the diagram. The use of the term "Computer based systems" in Figure 3 is confusing because the examples used for "Sensitive digital assets" are inclusive of "Computer based systems." Considering that Figure 3 was adapted from the equivalent figure in IAEA Nuclear Security Series No. 42-G (Computer Security for Nuclear Security), a better approach would be to simply refer the readers to this IAEA reference for additional information regarding security	X	Thank you for the very detailed explanation, the intent is fully accepted as the current (b) has emerged through attempts to resolve several comments concurrently. Wording has been proposed as an alternative under the basis that the relationship needs to be a little clearer as: i) NST070 still needs to cover the security of non-computer based sensitive information assets which we don't want to unintentionally equate the full set of which with computer security; ii) The Figure needs a textual reference; and iii) NSS 42-G/17-T Rev. 1 deal with the security of non-sensitive digital assets to provide for a DCSA to protect SDAs The proposed wording as drafted is as follows: (b) Security of sensitive information assets (e.g. information storage, processing equipment, and computer based systems). Detailed guidance on the security of computer based systems and sensitive digital assets can be found in Ref. [6] and Ref. [8]. 2.30. The relationship between sensitive information and sensitive information assets is depicted in Fig. 3.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
						of sensitive information assets, in lieu of adapting the figure and associated concepts in NST070.				
NSGC	United Arab Emirates	FANR	2	3.9, 3.10,3.11,3.12,3.13	Add example of: What are the common penalties or regulatory requirements imposed by member states in these situations?	To clearly identify the type of the penalty.	X			
NSGC	United States of America	NRC	7	4.3	Add something like, when information is being classified, consideration should be taken to understand that a piece of information by itself may not be sensitive (or the consequence of compromise of the information is not high), but it, along with other pieces of information may have		X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					severe consequences. Therefore, when taking a graded approach, the potential sensitivity of combined pieces of information need to be considered.					
NSGC	Australia	Vanessa Robertson	7	4.9	(1) Secret (2) Protected (3) Official: Sensitive or Official-Use-Only	Has the IAEA done a survey of Member States to see what countries use for classification of sensitive information? "Confidential" is a marking that is often used by businesses when sending personal information. In this context, it is used based on the common-usage of the word "Confidential". However, it does greatly complicate the use of "Confidential" as defined by the State given the different storage/handling/legal requirements.			X	The list is given as examples only. Confidential is well understood and established aspect of both State and organisation-specific approaches to classification schemes. It is proposed to stick to the original list as it was published by consensus in the original publication of NSS 23-G, changing the list now would also need to be reflected in Annex I, including the existing impact statements per each classification which have been previously published by consensus.

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Egypt	Prof. Wael EL Gammal	3	4.11	Classification schemes for sensitive information have traditionally been designed in response to the potential impact of a loss of confidentiality. A classification scheme developed to focus equally on the confidentiality, integrity and availability of sensitive information could adopt one or a combination of the following approaches:(a) Extending the use of established classification labels (e.g. secret) to encompass all aspects of confidentiality, integrity and availability. This is a simple solution, but it lacks specificity to inform the selection of information security measures.(b) Implementing a more complex scheme, where each level separately indicates the degree of confidentiality, integrity and availability. For example, an information object might be classified as 'Secret-C, Confidential-I, Restricted-A' to indicate different requirements for each security aspect. This provides precision but increases complexity.(c) Utilizing technology to manage complex classifications. Modern information management systems can enforce multi-dimensional classification schemes while presenting simplified interfaces to users, reducing the burden of complex manual classification.Regulated entities should explicitly document in their information security management system how integrity and availability requirements are derived from the overall classification level.	The original text mentions the possibility of addressing all three information security aspects but doesn't provide sufficient practical guidance on implementation. The proposed text offers concrete examples of multi-dimensional classification approaches and acknowledges the role of technology in managing complex classification schemes, making the guidance more actionable.	X	Examples have been taken from (b) and (c).		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
TRANSSC	Japan	NRA	6	4.15(c)	Examples of information that could be identified as sensitive information that is classified and handled in accordance with information security measures [9], includes information in the following categories: (a) …; (b) …; (c) Information relating to the quantity and form of nuclear and other radioactive material in transport*; (d) …; ------------------------------------- * Such information may be displayed on the transport packages for safety by the national/international transport regulations. Interface between security and safety should be considered (para.3.20 - 21).	Trasport is carried out in public domain and the information such as quantity (Bq) or form (UN numbers) is valuable for workers (public) or first responders in incidents/accidents to judge the potential risk of the contents. The displays (labels or placards) are required by the transport regulation. Therefore, the interface is important, and this information should be added (in a footnote).	X			
NSGC	Australia	Vanessa Robertson	8	4.15 point (a)	(a) Details of physical protection systems, computer security measures and any other security measures established for nuclear material, and other radioactive material, and associated facilities and activities, including information on protective security overlay, Command, Control and Co-ordination (C3) procedures, capabilities, static and mobile response forces and arrangements relating to transport security;	Provides broader detail on information that could be deemed sensitive information, which is relevant to the overall protective security overlay	X	The proposal has been adapted to be more in line with IAEA guidance terminology, as original drafted it now reads: *...including information on the performance of physical protection elements, command and control procedures, guards and response forces and arrangements relating to transport security;*		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Australia	Vanessa Robertson	9	5.5	In the sentence after 'This process includes…' include an additional sentence: 'The value of the information to adversaries can be measured by the level of harm the information could cause relative to the Design Basis Threat, threat or vulnerability assessments.'	The Design Basis Threat, threat and vulnerability assessments provide a great measure of how sensitive the information may be, relative to how it could be used for an adversary to defeat a nuclear security plan.	X			
NSGC	Finland	Paula Karhu	2	6.5	Modify: "[The] information security [management system] should be part of ~~integrated with~~ the regulated entity's ~~other~~ integrated management system~~s (e.g. for safety, quality, physical security and computer security) in a coherent manner, forming an integrated management system~~ to ensure a holistic[, balanced, and risk-informed] approach to overall management."	The idea is to have one integrated management system. It is an established term. QM etc. functions do not have to be considered as separate management systems (while admittedly, as per ISO/IEC 27 000, ISMS does). Computer security is part of information security (NSS 42-G), so it cannot be listed separately as in the present version. Brackets indicate an alternative proposal.	X			
NSGC	Japan	NRA	5	p.37, Para. 6.50, 2nd line in this para.	Suggest changing the word of "escalated" to be, for example, "communicated"	It seems that "escalated" may not be an appropriate word in the context of the para. 6.50.	x			
NSGC	United Arab Emirates	FANR	3	6.5	Suggest explicitly encouraging integration with safety, quality, and physical protection management systems via shared governance models and audit protocols.	To ensure the full integration of information security management system.	X			
NSGC	Japan	NRA	2	p.32, Para. 6.16, The last phrase in this para.	Suggest changing the phrase to be "~~the integration of~~ information security should be 'an integral part' (or, 'an essential element') of ~~into~~ nuclear security culture programmes to ensure ~~contributes to~~ the sustainability of nuclear security."	The phrase "integration of information security into security culture programmes contributes to the sustainability of nuclear security" is an oversimplification, suggesting that "incorporation alone will achieve sustainability". Instead, we suggest changing it to be "information security should be 'an integral part' (or, 'an essential element') of nuclear security culture programmes to ensure the sustainability of nuclear security".	X	Removed the reference to 'essential element' to avoid confusion with NSS 20.		
NSGC	Japan	NRA	3	p.33, Para. 6.23. (f)	Remove the highlight on the word of "subordinate".	Minor editorial. It is not clear why the word of "subordinate" is highlighted.	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Japan	NRA	4	p.34, Para. 6.29, 3rd line in this para.	Suggest changing to be: "the contracting regulated ~~regulating~~ entity should ensure the following:"	Minor editorial	X			
NSGC	Australia	Vanessa Robertson	10	6.33	… Such systems should be capable of identifying unauthorized, or unusual (i.e. large volume, unexpected time of day), sensitive information transfers (i.e. a data loss prevention).	In some cases, standard authorisations occur. An insider could use a standard authorisation to obtain information so additional "flags" would need to be used for detection/alert. An unusual sensitive information transfer may occur at an unusual time of day (when a worker is not rostered on), or be a volume of information larger than normal.	X	Added unusual with examples (rather than i.e. as non-exhaustive) before unauthorised to avoid confusion as both examples may be unusual but authorised and leave DLP to be focused on the prevention of unauthorised. Currently drafted as follows:6.33. Independent, non-repudiable systems should be used to detect and alert on insider activities. Such systems should be capable of identifying *unusual (e.g. large volume, unexpected time of day) or* unauthorized sensitive information transfers (i.e. data loss prevention).		
NSGC	Australia	Vanessa Robertson	11	6.45	… The incident response plan should be subject to continual improvement, based on feedback from DBT exercises, drills, …	It would be good to have a specific reference to DBT exercises. A DBT exercise is generally much larger/more complex than standards drill and normally includes the regulated entity, regulators, law enforcement and other agencies. Improving the incident response plan based on DBT exercises and feedback received from internal and external representatives helps make the incident response plan more robust.	X	As NSS 23-G is a cross-cutting document and a DBT might not apply to all covered domains, exercises have been added without the DBT exercise limiter.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	United States of America	NRC	6	2.5, 2.6, 2.7 and Fig 2.	In general, the definitions of information and information object used here are more closely aligned to the concepts of 'data' vs 'information'. Data is raw, unprocessed facts and figures, while information is data that has been organized and processed to provide context and meaning. In fact, NIST defines information as "Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. An instance of an information type." So, the definition of information used here does not align with the definition of information that is more generally used.	Consider better clarification and relationships between concepts such as data, information, information objects, and information type.			X	This is well recognised and has been heavily debated during the drafting of the document. The terms have been established within the NSS in a way that aligns with the established usages in the CPPNM/A, ICSANT, and INFIRC 225 and have received consensus publication in NSS 20, 13, 42-G, 23-G, and 17-T Rev. 1, et. al. This publication, as a revision of NSS 23-G, risks being misaligned with the series and/or not supporting adherence to international instruments if the terms are reconsidered at this level.
NSGC	Australia	Vanessa Robertson	6	Fig. 5		"URC C", "URC B" and "URC A" need to be defined. How do these three URC's relate to the concept of URC in other IEA publications?	X	URC A, B, C were published in the original version of the diagram by consensus in NSS 42-G. The State is responsible for defining URC, HRC, and any subdivisions thereof. As this may be confusing the subdivisions were removed from the diagram.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Russian Federation	Rosatom	1	General	It is necessary to change the content of the document in accordance with its Document Preparation Profile.	According to the aim of revision of this publication, as declared in the Document Preparation Profile approved by the results of the 21st NSGC meeting, «*Much national and international guidance exists regarding the establishment and management of information security frameworks for information of various types, in the form of both high level guidance and detailed standards. This publication does not intend to replace such guidance*». The presented version of the document, in comparison to the current edition of NSS 23-G, largely addresses the issues of national information protection regimes, and not the issues of nuclear security. Such issues are beyond the competence of the IAEA, the NSGC and the Nuclear Security Series in general, and should not be examined in this publication.	X	Accepted. NS is a state responsibility and the existing publication of NSS 23-G may have provided guidance that could focus more on wider national information protection regimes. For example, consider the following consensus language from the existing NSS 23-G that has been redeveloped in NST070 to be less prescriptive: 3.8. State policy on the security of information should define which type of information the State wishes to be secured and indicate how that security is to be applied. This is usually set out in a security manual compiled by the State’s national security authorities (or other appropriate authority). **A manual of this sort may not make any direct mention of sensitive information for nuclear security. ...** 3.16. A national system of classification should be established and maintained to group information into classes .... **This should be a national system, not specific to a particular industry or devised by a single facility**. In many instances, ... NST070 has removed the sole focus on national information protection regimes and provide greater flexibility for the application of State responsibility in nuclear security. The start of Section 3 was drafted to make it apparent that the described elements, for nuclear security, can be addressed as the State chooses within its legislative and regulatory framework. In comparison the section 'framework for securing sensitive information' in the existing consensus NSS 23-G would have only applied to national information protection regimes. To address this comment, the proposed response to RUS.2 further clarifies the distinction between wider and regime-level information security policy frameworks for nuclear security. It also includes specific statements to ensure the coherence of existing national frameworks is preserved. This is proposed as consistent with both the DPP approved objective (i.e. bridging the gap between national frameworks and standards while		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
								describing the elements necessary for effective nuclear security) and the existing consensus publication of NSS 23-G.		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Russian Federation	Rosatom	2	General	Exclude consideration of information protection regime issues (e.g. in Section 2, Section 3, Section 4, Section 5).Within the competence of this publication, it is possible to consider issues of computer security and the security of information related to nuclear facilities.	The issues of establishing, developing and maintaining national information protection regime, including the content of the national legislative framework for information security, designation of the competent authority responsible for information security at the national level, its functions and authority, defining sensitive information classification criteria, its structure and content, the order and the scope of its disclosure and the order of its handling are defined by each State.The issues of information security not related to nuclear materials and nuclear facilities are beyond the competence of the IAEA and should not be considered in this publication.Select paragraphs (including, but not limited to para 3.1, 3.2, 3.9, 4.6, 4.10, etc.) oblige the State to standardize approaches in relation to information security without reference to nuclear security regime, which is a limitation and does not correspond to the nuclear security approaches in the form of «best practices».	X	Accepted with thanks for the detail in the comment. The phrasing in the highlighted paragraphs concerning 'sensitive information' has historical precedent from the current consensus publication of NSS 23-G (where, for example, the quoted 3.1 and 3.2 are directly taken from consensus text with only minor editorial modification).In those instances, the specific definition of 'sensitive information' within NSS 20/Nuclear Security Series (NSS) was relied upon to provide the necessary limitation to nuclear security:'sensitive information. Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.'In accepting the comment paras. 3.9, 4.6, and 4.10, and Fig. 7 have been modified to clarify application to nuclear security and avoid wording that may inadvertently led to a less flexible interpretation. New wording has been proposed at the start of Section 3 to do the following:1) Provide initial qualification that this is specific to sensitive information within the nuclear security regime;2) Describe a State's overall framework as a "national information security framework";3) Highlight that if such a national framework is deemed authoritative for the nuclear security regime requirements necessary for nuclear security should be implemented in a manner that is coherent with both the nuclear security regime and the existing national information security policy framework (previously it was only one-directional).4) Note that there are instances where extending a national policy framework may not be ideal and that a nuclear security regime specific framework may be desired.The new paragraph for (4) reads:3.6. In instances where the State’s national information security policy framework is deemed by the State to not be sufficiently comprehensive for nuclear security, not directly applicable, or if a more focused approach is preferred (e.g. to provide more effective concurrent oversight of both governmental and commercial entities), an information security policy framework should be established		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
								specifically for the nuclear security regime falling under the purview of the competent authority for information security in coordination with the national security authorities (hereafter 'information security policy framework' refers to either the supplemented national framework or a framework established specifically for the nuclear security regime).		
NSGC	Russian Federation	Rosatom	3	General	It is necessary to change the title of the document to «Security of Nuclear Information (Revision 1)».	It is necessary to change the title of the document to «Security of Nuclear Information (Revision 1)», because it more accurately represents the stated content of the document and matches the wording "security of sensitive information", in accordance with NSS 42-G, NSS 20 and the Fundamental principle L of A/CPPNM. In addition, the titles of the documents in the Nuclear Security Series follow the principle of naming as «Previous title (revision 1)».			X	The documents title was proposed for modification and accepted with the approval of the DPP. This was presented to all Security and Safety committees and accepted with the following three primary basis: 1) NSS 42-G was published as "computer security for nuclear security" rather than "security of computer based systems" so "information security for nuclear security" provides functional and stylistic parity; 2) NSS 23-G in the existing publication states in Objective "This publication provides guidance on implementing the principle of confidentiality and on the broader aspects of information security". 3) "Security of Nuclear Information" is not accurate to the content of the document as there will be much non-sensitive nuclear information that doesn't fall under the purview of information

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
										security; and 4) "Nuclear information" does not convey the cross-cutting nature of the document as it is not defined and may provide an impression that it only covers the scope of nuclear material and nuclear facilities rather than the broader scope of nuclear security required for cross-cutting guidance. Historically many publications in the NSS have changed titles when published, for example: 1) "Security in the Transport of Radioactive Material," was revised and issued in 2020 as No. 9-G (Rev. 1) with the slightly altered title, "Security of Radioactive Material in Transport." 2) The 2009 Implementing Guide known as "Development, Use and Maintenance of the Design Basis Threat" (NSS No. 10) was significantly revised. Its 2021 version, No. 10-G (Rev. 1), is now titled "National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements," reflecting a broader approach to threat assessment. 3) The Technical Guidance document originally published in 2010 as "Educational Programme in Nuclear Security" (NSS No. 12) was updated and re-titled in its 2021 revision (No. 12-T (Rev. 1)) to "Model Academic Curriculum in Nuclear Security." 4) The original Technical Guidance, "Computer Security for Nuclear Facilities" (NSS No. 17, published in 2011), was revised and re-issued in 2021 as No. 17-T (Rev. 1) under the title "Computer Security Techniques for Nuclear Facilities."
NSGC	Russian Federation	Rosatom	4	General	Exclude the connection with nuclear safety and accounting and control of nuclear materials (starting from para 2.18 and further).	The publication aims to provide guidance on the handling of information regarding nuclear security. Issues of nuclear safety and accounting and control of nuclear materials are not integral components of nuclear security.			X	The documents title was proposed for modification and accepted with the approval of the DPP. This was presented to all Security and Safety committees and accepted with the following three primary basis: 1) NSS 42-G was published as "computer security for nuclear security" rather than "security of computer based systems" so "information security for nuclear security" provides functional and stylistic

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
										parity; 2) NSS 23-G in the existing publication states in Objective "This publication provides guidance on implementing the principle of confidentiality and on the broader aspects of information security"; 3) "Security of Nuclear Information" is not accurate to the content of the document as there will be much non-sensitive nuclear information that doesn't fall under the purview of information security; and 4) "Nuclear information" does not convey the cross-cutting nature of the document as it is not defined and may provide an impression that it only covers the scope of nuclear material and nuclear facilities rather than the broader scope of nuclear security required for cross-cutting guidance. Historically many publications in the NSS have changed titles when published, for example NSS 9-G Rev. 1, NSS 10-G Rev. 1, NSS 12-T Rev. 1, and NSS 17-T Rev. 1.
NSGC	Russian Federation	Rosatom	5	General	The text needs to be updated in order to establish a clearer relationship between the recommendations of NST070 and NSS 42-G	The draft NST070 states that computer security is a part of information security. Thus, the recommendations and approaches of NST070 apply to NSS 42-G. At the same time, NST070 provides for the development of a management system, policies and other documents that are not mentioned in NSS 42-G. For example, NST070 states the need to develop a separate "incident response plan" (paragraph 6.42). At the same time, the NSS 42-G publication states that "contingency plans" should take into account computer incidents, i.e. recommendations for the development of a "computer" plan are not provided. It is important that the user of the NST070 publication has a clear understanding of where information security approaches are discussed in general, and where specific measures are provided (for example, which depend on the type of storage and	X	Accepted. As NSS 23-G/NST070 are cross-cutting documents it is important to note the following is the list of areas where contingency plan is addressed within the NSS and other related instruments: •NSS 13 – (Singular per State/facility) Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts. •NSS 20, 14 – Uses ‘response plan’ and ‘contingency measures’, not defined •NSS 15 – Uses ‘national response plan’ •A/CPPNM – used, not defined •CoC – uses ‘response plan’ (in the context ‘appropriate response plans’), not defined The use in NSS 42-G implies that the computer security programme, which exists within each organization, provides multiple contingency plans which is counter to the singular contingency plan described in NSS 13. Consider the following clauses from NSS 42-G:		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
						use of information – on paper or in a computer system).		•8.24. The CSP should include contingency plans to respond to cyber-attacks. These plans should take account of the possibility of insider and blended attacks. The contingency plan should identify specific types of computer security incident and the required response to these incidents. •8.25. When a computer security incident is also a nuclear security event, the relevant contingency plan should be activated. This may form part (i.e. a predefined set of actions) of the singular "contingency plan" in nuclear facilities while being more broadly applicable to other areas of nuclear security. To address the specifics of the proposal 6.42 and 6.44 have been redrafted as follows: •6.42. While this section provides the overall framework for information security incident response, additional guidance on technical aspects of computer security incident response specific to nuclear facilities can be found in Appendix 1 of Ref. [9]. •6.44. A designated team within the regulated entity should establish and document the elements necessary for an effective response to information security incidents. These elements may be formally documented either as a dedicated, standalone incident response plan, or as an integrated section within another relevant response plan such as a contingency plan. This plan should do the following… To address the more general intent of the proposal "Elements…" has been removed as a subheading, the second level subheadings have been promoted so they appear as the elements, and the following text has been added to the start of Section 6: •6.1 … With the widespread use of computer based systems within the creation, processing, and utilization of sensitive information, many of the elements of an information security		

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
								management system described in this section may be addressed wholly or partly within a subordinate computer security programme as detailed in Ref. [8]. It is proposed that the balance of Section 6 represents good practice for information security management system regardless of implementation for computers or other forms of information.		
NSGC	Russian Federation	Rosatom	6	General	Provide a definition of the term "regulated entity"	This term is not used either in the high-level publications of the NSS or in the current version of NSS 23-G, but it is the main one in the draft NST070. Without understanding meaning of this term, consideration of the NST070 is impossible	X			
NSGC	Russian Federation	Rosatom	7	General	Throughout the draft NST070 instead of «regulated entity or competent authority» use «competent authority or regulated entity»	The sequence “State – competent authority – operator” is used in the logic of IAEA publications of the NSS Series	X			
NSGC	Finland	Paula Karhu	1	General	Thank you for resolving so many comments effectively.	Feedback	X			
NSGC	Russian Federation	Rosatom	10	Annex I, para I-6, d)	Exclude examples	Examples relate to nuclear weapons	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Egypt	Prof. Wael EL Gammal	4	Annex II	(Add to Table II-1, under Section 4 - IT Systems and Computer Systems, a new subsection): "4.4. Advanced cyber threats A. Information about zero-day vulnerabilities or unpatched security flaws in computer systems handling sensitive information [II-1], [II-2], [II-4] - Confidentiality - Such information could enable adversaries to compromise systems before security patches are available. B. Details about supply chain security verification processes and results [II-1], [II-2], [II-3] - Confidentiality - Information revealing how a facility verifies the integrity of its supply chain could enable adversaries to bypass these controls. C. Information about advanced persistent threat (APT) detections or indicators of compromise [II-1], [II-2], [II-3] - Confidentiality, Integrity - Knowledge of detection methods could help adversaries evade security monitoring systems.	The original examples in Annex II cover traditional information security concerns but could be enhanced with examples reflecting modern cyber threats that particularly impact nuclear facilities. The proposed additions provide concrete examples of emerging digital threats that should be considered sensitive, helping regulated entities better identify and protect against contemporary attack vectors.	X			
NSGC	Australia	Vanessa Robertson	13	Annex II, 13.	Column 1 – 13.5 Details of vulnerability assessments Column 2 – [II-1] Column 3 – Confidentiality Column 4 – An adversary could use information on vulnerability assessments, especially those identified but yet to be addressed, as a point of exploitation.	Once a vulnerability assessment has been completed, the risk of the areas of identified vulnerability being exploited becomes higher until such time as security measures are adjusted to reduce/remove the vulnerability. An adversary, especially an insider threat, could utilise this window to target weaker/compromised security.	X			

Committee	Country	Reviewer	Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC	Australia	Vanessa Robertson	12	Annex II, 2.1	Column 3 – Integrity and Confidentiality Column 4 – "… of nuclear material. Details of this nature could be of great use to adversaries who wish to know the location, quantity, type, form of nuclear material or other radioactive material to identify best material to sabotage or steal."	Information on the location, quantity, type and form of the material would be of high interest to an inside/outside threat looking to sabotage or steal material.	X			
NSGC	Egypt	Prof. Wael EL Gammal	5	Annex IIIInformation Security Training ProgramCapacity Building Program	In addition to an information security training programme, there are a number of other methods by which security awareness messages can be transmitted...III-10. Measuring Training Effectiveness and Continuous ImprovementThe regulated entity should implement metrics to evaluate information security training effectiveness and adapt content accordingly:(a) Pre and post-training assessments to measure knowledge acquisition; (b) Simulated phishing and social engineering exercises with tracking of success rates over time; (c) Periodic spot checks of security practices (e.g., clear desk audits, password compliance); (d) Analysis of security incident reports to identify potential training gaps; (e) Role-specific training effectiveness metrics tailored to different security responsibilities.Results should be analyzed quarterly to identify trends and adapt training content to address emerging risks and observed compliance gaps. Different training approaches should be developed for personnel with specialized security roles versus general staff.	The original text provides good training content but lacks guidance on measuring effectiveness and adapting training over time. The proposed addition provides specific metrics and methods for evaluating training impact and tailoring content to different roles, enhancing the sustainability and continuous improvement of information security training programs.	X			