Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
NSGC — Japan/The Nuclear Regulation Authority (NRA)							
1.	Para 2.22./Line 5 & 8	Replace "physical protection plan" with "security plan" (2 places)	Align with terminology used in NSS No. 13 (as that used in para 2.31.)	X			
2.	Para 2.23./Line 5	Suggest using another word: "the adversary can ~~adversely impact~~ compromise functions….)	Try to avoid using "adversary" and "adversely" together in one sentence.	X	Adversely impact is commonly used. But in this instance propose accepting and changing to "negatively".		
3.	Para 3.21	Suggest that specific examples be provided.	Concrete examples will make it easier to understand.	X			
4.	Para 4.6. (i)	Suggest that it be rewritten to make it a little more understandable.	For the reader to easily understand this paragraph.	X			
5.	Para 6.4./Line 4	Remove "as" and insert "." soon after "a 'plan, do, check, act' cycle" and before "This".	Minor editorial	X			
6.	Para 6.30./Line 3	Remove "[]".	Not clear why "nuclear material," is in brackets.			X	It is a direct quote from the source reference NSS 8-G where the brackets appear in the original text.
7.	Para 6.39./Line 2	Change "authorized" to be "unauthorized"	Assume it is a typo.	X			
NSGC — Saudi Arabia							
1.	1.7/3	1.7. The terms used in this publication are to be understood as explained in the IAEA Safety and Security Glossary……	The IAEA Safety Glossary has been changed to IAEA Safety and Security Glossary.	X			
2.	1.10/(a)	Establishing effective state legislative and regulatory ~~policy~~ frameworks for maintaining the confidentiality, integrity, and availability of sensitive information;	The document is implementing guide. Its scope should stick to Recommendation level documents. Regulatory framework is important aspect for the information security.	X			
3.	1.15	The intended audience for this publication is all those who are responsible for the security of sensitive	Response organizations should be part of the list of intended users of this publication.	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		information, for example, competent authorities, including regulatory bodies; management in facilities, companies or organizations involved in the use, storage or transport of nuclear material or other radioactive material, response organizations in case of nuclear or radiological emergencies……..					
4.	Fig 3	Should include examples from nuclear business like NMAC, Storage locations, Targets in facilities etc….	The examples are from general computer security or information security. Specific examples from nuclear material and nuclear facilities will be more useful.	X			
5.	3	Same as comment 2 above.		X			
6.	3.13		There is not much guidance in 29-G on regulating Information security. In this implementing guide more guidance is needed to be included.	X	Guidance has been expanded on during the review of comments as appropriate.		
7.		Overall document is in very good shape and provide sufficient guide at State level. Some specific guidance with examples should be added based on IAEA recommendation level documents.		X			
NSGC — Islamic Republic of IRAN/ National Nuclear Safeguards Department (NNSG)							
1	2.2	Information security is the preservation of the confidentiality, integrity and availability of information in any form.	Based on NSS 23-G, information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts,	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			events, processes, thoughts, facts and patterns.				
2	2.4/FIG.1(The third box from the top)	Implementing an effective information security management system at the organization level to ensure the security of the sensitive information.	The management system is related to a more general scope in an organization and thus should be limited to the information security scope.	X			
3	2.5	An information object is “knowledge or data that have value to the organization” [2] referring to any digital or physical items containing sensitive or classified information related to nuclear materials, facilities, or activities. Information objects can be 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 information.	It should be necessary to define information object in detail.	X	The proposed addition implies information objects are sensitive. However the paragraph is describing what an information object is without consideration of sensitivity. Preserved “physical or digital”.		
4	3.16/2	The State should ensure that each identified entity has defined and assigned responsibilities & authorities and falls under the oversight of the appropriate competent authority for information security in the nuclear security regime.	The term “authorities” is essential for conducting Responsibilities.	X	Moved appropriate Infront of responsibilities. Now reads as: assigned responsibilities, appropriate authority and falls under the oversight of the competent authority…		
5	3.19	Regulated entities and competent authorities engaging third parties are responsible for	It is necessary to define and develop an evaluation mechanism in order to ensure	X	Prefixed monitoring and evaluating with “for”		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		developing contractual requirements for maintaining information security in adherence to the State's information security policy framework and monitoring and evaluating the performance of the third parties to ensure compliance with the contractual requirements.	compliance with the contractual requirements.				
6	6.28.	A system should be in place to control why, when, to what extent and how specific individuals are authorized to have access to, or the ability to modify, sensitive information and sensitive information assets.	According to security principles it is necessary to limit the amount of information that individuals have access to.	X			
NSGC — Cuba/Directorate of Security and Protection							
1.	Art. 2	It is suggested to add, in an article, after 2.27 that refers: "If a certain Information that was not initially conceived by the state information security regime as sensitive, and even not by the competent authority or by the regulated entity itself and that may have a certain sensitivity for the nuclear technological or physical security regime and the accounting and control of nuclear material, at some specific moment in the process, this information must be protected in accordance with its importance, in order to	Clarify, Add	X	Propose inclusion of clarification in 2.27 with the following text: "information and be re-evaluated if a previously unknown consequence comes to light, as this could significantly amplify the impact"		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		maintain its integrity, reliability or availability, as appropriate.” Example, in areas of armed conflict, etc.					
2.	Art. 5.7	Section 5.7 states that “Secure transmission protocols should be established to protect sensitive information from compromise. For instance, secure network channels or communication methods utilizing cryptography can be employed to ensure that information remains protected during digital transmission". It is suggested to add that: “not only during digital transmission, but also during transportation on mobile devices or other forms of data storage and/or transmission”	Clarify, Add	X			
NSGC — ENISS							
1	General comment	The draft concerns the arrangement at state level for sensitive information but some arrangements could be completed by nuclear operators with specific measures and a specific classification of sensitive information. Only State’s nuclear security regimes are concerned but not operators’ organisation while they could have other security measures related to sensitive information. Regulatory requirements at State level should be limited to very high		X	The document outlines a consolidate approach to State information and that generated within operation of a facility/activity. The exact classification of the information remains a sovereign decision.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		sensitive information and for confidentiality reason (very secret, secret, restricted).					
2	General comment	Regulation should concern only sensitive information related to nuclear security and NMAC and only for confidentiality reason. These information shall be regulated because their dissemination could have harmful consequence on the State and the Nation. However sensitive information for integrity and availability reason has impact on nuclear safety and, in that sense, they are under the responsibility of the nuclear operator (nuclear operator is responsible for nuclear safety of its facilities).		X	The draft, as the previous revision of NSS 23-G did and NSS 42-G, highlights and addresses concerns for nuclear security from the compromise (confidentiality, integrity, and availability) of sensitive information and sensitive information assets. A criminal or other intentional unauthorized act against a information processed by a system important to nuclear safety could lead to a nuclear event and is therefore within the scope of guidance.		
3	General comment	The draft doesn't specify who is responsible for the sensitive information and in charge of its classification. The notion of information owner should be defined.		X			
4	Title	The title should be written as follows: Information Security for Nuclear Security, Nuclear Safety and NMAC	The title of the draft mentions only nuclear security while the document concerns not only nuclear security but nuclear safety and NMAC as well			X	NMAC is included in nuclear security, the focus of the document is on nuclear security and doesn't provide guidance on nuclear safety aspects (e.g. reliability of information)
5	§2.3	Remove "maintain nuclear safety"	Nuclear Security contributes to nuclear safety but nuclear safety issues are specific. Sensitive information related to nuclear security shall be regulated within the State's security regime but information related to nuclear safety should not be regulated because nuclear	X	Adapted to highlight safety functions that rely on sensitive information.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			operators are responsible for the quality of these information (integrity and availability). Operators should also define their own requirements for technical information that contribute to nuclear safety. Measures to guarantee the integrity and the availability of technical information necessary for safety reason should be defined by the operators.				
6	2.18		The paragraph mentions sensor values that are used to control reactivity. These types of information are technical and they are also under the responsibility of the operator. This kind of information shall not be regulated in so far as it doesn't concern nuclear security with risk of dissemination of sensitive information.			X	Per resolution to ENISS #2 the document provides guidance on information which if compromised (CIA) could lead to a nuclear security event. The example in 2.18 is informative and fits within the approved scope of the document and previously published consensus guidance.
7	3.23	The State's information security policy framework should define criteria that should be applied by regulated entities to identify the information that the State wishes to protect (…)	Type of information is not clear. All information that contribute to nuclear security or NMAC should be considered. It's important for the State's security regime to establish criteria to classify this information regarding their integrity, their availability and their confidentiality.	X	Modified as "criteria necessary to identify the information " as some State's may define the exact information that needs to be protected for some industries and the criteria to identify may not be applied.		
NSGC — France/Department of nuclear security -Ministry of Ecological Transition							
1.	1.7	Add "and Security" 1.7. The terms used in this publication are to be understood as explained in the IAEA Safety and Security Glossary [2],	Forgotten	X			
2.	2.18	Sensor values that are used to ~~control~~ **ensure** nuclear **safety function** reactivity,	From the point of view of nuclear security, loss of control is not very sensitive if safety is	X	Used "ensure the nuclear safety function to control reactivity" in both instances.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		for example, are likely to be considered sensitive information. Sensitive information could also describe vulnerabilities that an adversary could exploit to undermine those functions. For example, the sensor values that are used to ~~control~~ **ensure nuclear** reactivity **safety function**.	still ensured (by dedicated sensors). It would result in the denial of use of the reactor, which is a problem for the operator, but maybe not for the State (depending on the State nuclear security objectives). But ensuring a safety function is, in all cases, a nuclear security objective. Moreover, security experts may not all know that nuclear reactivity is a safety function.				
3	2.19	it can prevent the individuals or information assets from correctly performing their functions, **and it could lead to nuclear accidents.**	To emphasize that availability and integrity can be very important.	X	expanded with the following wording: …and potentially lead to a nuclear security event or a nuclear accident.		
4	2.20	(a) Information relating to the control of important physical processes relevant to nuclear security **and safety;**	In particular integrity and availability.	X	"Nuclear security and its interfaces with nuclear safety"		
5	2.32	2.32. Gaps or deficiencies in one security domain can affect the security of other domains, and so it is essential to adopt a comprehensive approach that considers all these domains. Legislative and policy frameworks for securing sensitive information should also consider the need to ~~balance security objectives with~~ **take into account** other objectives, such as operational objectives, transparency and safety and **provide adequate measures to do so.**	Security objectives should not be reduced because of other considerations. But, if it is not possible to achieve these objectives along with other important objectives, the legislative and policy frameworks should make sure that an adequate decision can be made.	X			
6	3.1 and 3.2	Consider deleting, and begin at current 3.3	Repetitive, no new idea	X			
7	3.8	3.8. Legislation should ~~also be established to~~ define ~~the~~ **competent authorities in charge of controlling information security requirements and** sanctions or punishment		X	Removed requirements.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		that will be applied to individuals or organizations that breach ~~information security requirements~~ these requirements.					
8	4.7	4.7. A possible classification scheme for sensitive information, with classes that indicate the confidentiality of particular information objects, ~~could be determined on the basis of IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities, and~~ could contain the following levels **(see Annex I).**	Not clear how NSS 17 could be used. The idea that 3 levels can be used does not need it. Reference to Annex I could be more appropriate. If there is something else interesting in NSS17, the idea should be explained clearly.	X			
9	4.14	4.14. Some of the information in para. ~~4.14~~ **4.13** (e.g. personal information) could also be subject to specific security requirements under national laws not related to information security or could be subject to company policies.	typo	X			
10	5.1.1	Delete §	In France, use of “code words” is not allowed. It should not be part of an IAEA guidance, that should give good practices only.	X	Code words are currently in the pre-print of NST053 which will likely see publication as NSS 64-T before NST070. The content in 5.11 is providing practical considerations towards information security if they are used rather than advocating for their use. To make this clear the intent of the comment is accepted and the words “can effectively” have been replaced with “may. 55026681.pdf (iaea.org)		
11	Annex II, Table II, 3.1	Add “Confidentiality”	Along with “availability”, access to transport security plan, including transit routes, times and security measures, could help malicious acts	X			
NSGC — UAEA/FANR and Nawah							
1	2.25	Access to sensitive information, sensitive information objects and sensitive information		X	Clarified with: “…elements of the design and safe operation of a facility should be made aware of all sensitive information relevant to their tasking if this would…”		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		assets should be restricted to those individuals who have a genuine need for this access for the performance of their work. The dissemination of sensitive information should thus be limited to authorized individuals on a 'need to know' basis. However, the assessment to determine the authorized individuals who need access to sensitive information should be made taking into account other factors (e.g. safety considerations) that might introduce risks for the State. For example, individuals who should be made aware of all relevant sensitive information if this would reduce the risk to the State of a nuclear security event occurring	The example could lead to confusion that person responsible of design and operation shall have a full knowledge of sensitive information. In addition it is nor practical that a single person should be aware of all sensitive information.				
2	3.3 b	A legislative framework covering information security for sensitive information	The relevancy could be generalized in the state legislative for whole sector or general state wide not specifically related to nuclear security. Or to make it specific for nuclear regulator responsibility	X			
3	3.5	The State should identify and ensure coordination of all organizations having a role in the nuclear security regime, described in this publication as competent authorities, regulated entities, and third parties. Competent authorities create the regulatory requirements for sensitive information. Regulated entities have access to sensitive information within the nuclear security regime	To ensure coordination of states entities who are responsible of legislations related to information security. As it is covered under 3.15	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
4	4.7	A possible classification scheme for sensitive information, with classes that indicate the confidentiality of particular information objects, could be determined on the basis of IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities, and could contain the following levels or as defined by the state	Some states would have different categorization based on its legislations.	X			
5	Objective 1.9.	1. Adding the following sentence: Identify the storage media, for sensitive information all kind forms. 2. Reclassification of the sensitive information	1- In this strategic level identify the storage media for the sensitive information upon the category assigned Upon the time spending , usage , and the Country Privacy law	X	Attempted to address in 1.10 (b): (b) Identifying and classifying sensitive information and related information assets;		
6	Scope 1.5	• Adding waste management of Nuclear material or radiative source material sensitive information (life cycle)	Adding a cycle life of the nuclear and radioactive source material to be guarded. •	X			
7	**INFORMATION SECURITY CONCEPTS** 2.5	Adding tangible and not tangible sensitive information •	Adding to specify kind of the information's which been located as a tangible and not tangible.	X			
8	4.11	Add and inside of or	Giving access is can be conditional upon turnover of the organization or	X	4.11 appears to be an incorrect reference, addressed in 6.28(d)		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			promoting of personal who handling the information.				
9	6.25	For the 3rd party as a company and individual separately must be adhering to the low and Security policy	Example : as a company or 3rd party organization should apply for Security Clearness and individual also	X	A company cannot oblige a 3rd party company. This has been addressed in 3.19.		
10	Section 6.42 (C)	"Establish protocols for notifying and engaging internal and external stakeholders, (e.g. law enforcement and other relevant authorities)."	**It's a country specific** on how to handle an incident	X	Changed from should to could.		
NSGC — Finland/Stuk							
1	Para 1.5	Consider the definition quoted from ref. [2]: whether both "modification" and "alteration" are needed, and whether the words "or safety" should be added at the end of it.	For clarity and completeness. Alternatively, the difference between modification and alteration could be explained. Regarding the "and safety" – there could be a case of non-availability that would not compromise security but could compromise safety (e.g. in "pure" accident management).			X	The document attempts to answer the intent of the comment and recognises the problem expressed. However modification to the existing, additional explanation, or paraphrasing would not be appropriate for the Background section.
2	Para 1.6 and the following.	Add "…and safety" at the end of the sentence. Add a number to the following para.	Ensuring integrity and availability are very much serving the interests of nuclear safety. And they are part of information security.	X	The document is foremost focused on nuclear security and protection against malicious action. So modified to read "and its interfaces with nuclear safety" per DPP approved wording. Clarifying content is added to 2.3 and prior to that "nuclear security and its interface with nuclear security" is proposed for use.		
3	Para 1.10 subpara (c)	Add "and destruction" or modify: "Information security measures for the entire life-cycle of information."	For completeness.	X			
4	Para 1.11, line 4	Modify: "This publication complements existing ~~national~~ regulations, guidance, and ~~industry~~ standards."	ISO/IEC 27000-family is not national, nor strictly for industry.	X			
5	Para 1.12	Modify: "This Implementing Guide provides guidance on information security for nuclear security~~,~~ and ~~its interfaces with nuclear~~ safety~~, and with other elements of a State's~~	Same as in comment 2. And the rest of the sentence is part of nuclear security. For this reason the transport part of the next sentence is questionable (nuclear security covers transport security). The	X	The sentence was crafted to make it explicit that this should be perceived as a cross-cutting document so the three topics remain. Removed transport and the second reference to interfaces with nuclear safety however.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, and the detection of and response to nuclear security events.~~ This Implementing Guide will also address information security related to nuclear material accounting and control ~~and nuclear and other radioactive material in transport~~, as well as the interfaces of information security for nuclear security with nuclear safety.	interface in the second sentence has validity, if we consider the confidentiality/availability balance.				
6	Para 1.13, line 5, and in similar sentences elsewhere (e.g. 2.19, 2.20 (a), 3.3. (b))	"…but that is not considered sensitive in terms of nuclear security <u>or safety</u>,…"	Same as in comment 2.	X	Modified per comment #2.		
7	Para 2.3	"Protection against adversary actions that could affect the confidentiality, integrity, ~~and~~ <u>or</u> availability…"	Any of the three attributes/properties.	X			
8	Para 2.4	"… and <u>the information management system of</u> a regulated entity or competent authority~~'s information management system~~ should reflect the information security measures and activities necessary to support the nuclear security <u>and safety</u> regime, as some functions (e.g. the safe <u>and secure</u> operation of nuclear facilities) directly relevant to the State's nuclear security <u>and safety</u> objectives rely upon the confidentiality, integrity and availability of sensitive information" Text of Figure 1 should read "security <u>and safety</u> objectives".	The s-genitive did not seem to work very well (and if used, should have been added to the regulated entity as well). + same as in comment 2.	X	"Attaining the State's nuclear safety and nuclear security objectives ".		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
9	Para 2.13	Delete: ~~"However, information security measures can generally only be applied to information objects and information assets, in an effort to protect the relevant functions. 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 comprehensively in its tangible and abstract forms." or similar.	Information security measures are applied also to individuals (humans in Fig. 2). The second sentence is covered in 2.7.	X	Rather than the larger proposed modifications added individuals to the list.		
10	Para 2.28 (c)	Modify: "Where this equipment uses computer based systems, these are specifically referred to as sensitive digital assets, and the domain is referred to as computer security, …".	For clarity with respect to the following sentence.	X			
11	Fig. 3	1. The green box: Consider adding "e.g. Non-sensitive…". The grey box (SDAs): Modify: "e.g. ~~Desktop~~ Personal computers…"	1. Some of the data examples given in the green box could be sensitive (procurement data on suppliers, personnel data as pointed out in 2.20 (f)). To include laptops etc.	X			
12	Para 3.1	Modify: "…sabotage or of failure of detection or actions being undertaken to locate and recover…" or similar.	"Risk of actions" did not seem correct. And also detection probability can be affected.	X			
13	Para 3.27	Modify: "The competent authority for information security should also cooperate closely with the national security authorities, and[, as appropriate,] with the nuclear regulatory authority in order to devise the national	The regulator may be involved in the threat assessment process and in many countries is responsible for the DBT.	X	Propose "and other competent authorities in the nuclear security regime"		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		threat assessment or design basis threat."					
14	Para 3.28, line 2	The word "dedicated" should be omitted.	It is conceivable that an organization has one policy for quality, safety and security that includes information security. This is also allowed by ISO/IEC 27001.	X			
15	Para 4.13, the list	Add on the list information about the facility and its activities, e.g.: "Information on the facility and its operation the misuse of which could compromise safety." or similar.	There is also primarily safety or operations related sensitive information.	X			
16	Para 5.19, line 4	Consider adding: "such as information associated with national defence, security systems and measures, or private and personal information."	The list does not have to be exhaustive, but security is another example.	X			
17	Para 6.2, line 3	Consider adding: "The policy should articulate top management commitment in, and high level goals, objectives and requirements for information security."	As usual for policies. Objectives should be derivable from the policy.	X	"The policy should articulate high level goals, objectives and requirements for information security and represent management commitment"		
18	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, and to include physical security.	X	This was avoided as not all facilities/activities in a cross-cutting nature would have an IMS. So propose the following as I believe it fits the comments intent: This management system should be integrated with the regulated entity or competent authority's other management systems (e.g. safety, quality, physical security and computer security) in a coherent manner to ensure a holistic approach to overall management, such as an integrated management system.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
19	Para 6.5, line 3	Consider modifying: "…with the objective of ensuring confidentiality, integrity, and availability of ~~protecting~~ [sensitive] information.	Just "protecting" may not be understood to include the three objectives (which could be then deleted from the next sentence).	X	Wording modified to ensure the paragraph reads correctly as the two sentences are interrelated. 6.5. An information security management system is a regulated entity or competent authority's means of implementing systematic, structured information security measures and subordinate systems with the objective of protecting preserving the confidentiality, integrity, and availability of sensitive information. The system encompasses a comprehensive set of subordinate policies, procedures and processes (e.g. technical, administrative, and physical or other interconnected security measures) designed to preserve the confidentiality, integrity and availability ofprovide for the security of sensitive information, sensitive information objects and sensitive information assets.		
20	Para 6.5, line 4	Advise to delete: "subordinate ~~policies,~~ procedures and processes…"	Policy is a high-level entity, subordinate levels are managed by procedures etc.	X			
21	Para 6.22 (b), 8	Modify: "The personnel security process could ~~should~~ also include the signing of a non-disclosure agreement…"	The non-disclosure obligation may result directly from legislation without the need for an NDA, particularly for authority personnel.	X			
22	Annex II	Sensitivity column needs revision. The division of non-sensitive and sensitive can stay, but the division according to the CIA principles is questionable – if kept, it should be checked.	Availability of all sensitive information is important to someone (who needs it) or in some context (in a particular situation). Otherwise, we would not need that information. Integrity of most information is important, for decision making. If, after a re-check, all three principles are listed for every line in the table, it does not add value.	X	Understood but this would make the table impractical for inclusion. The further elaboration on the table in this revision was designed to reduce similar ambiguity from Annex II in the current NSS 23-G, during informal consultation within the NSS comprehensive review the secretariat was informed that the Annex was the highly appreciated and should be preserved for the revision. The following caveat has been added to II-3: The identification of whether an item is sensitive, the explanation, and the rationale are provided as non-exhaustive examples only.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
23	Annex II	9.1 heading, A. and B: Change the order: "Response and contingency".	Response plan is the primary one, contingency plan a plan B.	X			
24	Annex II	9.2: Change: "Security response plans…"	Same as above. We have response, and for it a response plan. Contingency plan may be added.	X			
25	General	The guide presents a thorough approach to and practical illustrations on information security.	General comment. The guide is long, however...	X			
NSGC — Russia/Rosatom							
1.	2.5	…and in other forms, visible view of protected systems itself, and channels for transferring information.	Here are presented the information in (on) storage means or in channels. But the other class of protected information is not presented: protected information may present protected system itself: visible view (appearance) of protected systems (including PPS), their elements (where they installed), or some produced fields. It can be the sensitive information.	X	In this context the information object would still be the document/system rather than the view. Added to 2.7 which now describes an information object as: (i.e. is tangible, can be labelled and is in the appropriate context, can be viewed)		
2.	2.16 and 4.2	**2.16.** It is important to note that an adversary could create or modify information, information objects and information assets for criminal or other intentional unauthorized purposes. ~~The latter could include attacks that are specifically designed and executed to mislead human or machine based decision making. This type of attack should be~~	Section 2 describes the concept. Specific recommendations are proposed to be indicated in the relevant sections. Thus, in clause 4.2 it is proposed to add item "c)" or include this case in item "a)"	X	Added to 4.2 as (b) The impact of of the compromise of the information's integrity or availability on the consequences of decisions made on the basis of the information, considering that the information made be targeted within an attack designed and executed to mislead human or machine based decision making.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		~~considered when protecting information on the basis of which decisions are made.~~ **4.2 …** **c)** The impact of the compromise of the information's integrity or availability on the consequences of management decisions (impacts) made on the basis of such information					
3.	2.18	… For example, the sensor values that are used to control reactivity might be converted using a calibration table, which is used in the case of multiple sensors that serve different purposes. If the calibration table is manipulated, multiple functions could be adversely affected, which means that ~~both~~ the sensor data, the calibration table <u>and</u> <u>calibration algorithm</u> should be assessed as sensitive information.	In the proposed example, an attack can also be carries out on the calibration algorithm (software libraries). This statement implies requirements for trusted software delivery and the implementation of a confirmation management process.	X			
4.	2.25	… The dissemination of sensitive information should thus be limited to authorized individuals <u>and</u> <u>sensitive digital assets</u> on a 'need to know' basis.	It is proposed to use the principle indicated in Fig.2	X	Used the "sensitive information assets" superset.		
5.	2.28	a) Security of sensitive information held, processed and communicated by authorized and unauthorized individuals <u>and</u> <u>sensitive digital assets.</u>	It is proposed to use the principle indicated in Fig.2	X	Used the "sensitive information assets" superset.		
6.	Below 2.28	Computer security is a particular aspect of information security that	To understand the general term "Information security", it is necessary to define its	X	Added alongside Finland/STUK Comment #10. Propose reducing the text during final editing.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		is concerned the protection of computer based systems against compromise.	components, including the term “computer security”. It is proposed to use the term, defined in “Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G” or redefine it using the term “sensitive information”				
7.	4.14	4.14. Some of the information in para. 4.13 ~~4.14~~	It should be the reference to previous para.– 4.13.	X			
8.	6.4* (below 6.40)	The regulated entity or competent authority should implement an information security incident management process, which includes 4 stages: - organization of work; - detection and registration of information security incidents; - response to information security incidents; - analysis of results.	For the purpose of a detailed description of the information security incident management process	X	Attempted to incorporate this into the incident response plan by the addition of a new (b) with other points believed to already be covered in clauses 6.4*: (b) Establish procedures for registering, recording, and tracking information security incidents, including the details associated with each incident and the response actions taken;		
9.	6.4* (below 6.40)	At the first stage: - creating conditions for effective monitoring of information security events; - appointing responsible persons and training them; - developing incidents response plans; - conducting training to handle incidents; - increasing staff awareness; - checking the integrity and availability of backup copies.	For the purpose of a detailed description of the information security incident management process	X	Addressed through inclusion in existing paras. With edits to 6.44, existing 6.41, existing 6.45. 6.44 now reads: 6.44. The information security management system should include security measures for the detection of suspicious activity, and for the alerting of monitoring personnel in an expeditious manner, for ensuring effective monitoring of the incident, and for verifying on an ongoing basis the integrity and availability of backups of information and information assets. An example of a detection security measure is a system that detects unauthorized exfiltration of sensitive information.		
10.	6.4* (below 6.42)	For an information asset or a group of similar assets, a private plan should be developed that contains:	For the purpose of a detailed description of the information security incident management process	X	This appears a little too detailed for an IG document and may apply primarily to digital assets. I would propose it should be considered in NSS 42-G/NSS 17-T Rev. 1.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		- technical description of the asset; - list of relevant information security incidents; - private measures taken on an asset to contain an incident, restore the asset and maintain or restore the production process it supports.					
11.	6.5	..(e.g. technical, administrative and physical security interconnected measures).	interconnected means, that the measures should work together. For example, if we install portal metal detector (technical measure), then we should place security guard (physical measure), who has and perform written instruction (administrative measure) how to work with metal detector.	X	Comment seemed to limit to physical measures. Suggest the following form to imply i) it's not just physical security interconnected measures as other could also apply to combinations of the former, and ii) allow for a consideration of other types of measures if existing: e.g. technical, administrative, physical or other interconnected security measures.		
12.	6.25	Add sentence. Certification of third party vendors by ISO or other National Standards in information security field is increasing level of trustworthiness.	Certified of third party vendors by ISO Standard (27001 for example), should increase the level of trustworthiness.	X	Accept the basis, but there was no earlier acknowledgement of standards in the normative text other than the diagram. Added a new paragraph 3.27 which would allow this trustworthiness to be verified as it may be addressed at the national policy level.		
13.	6.28	6.28 A system should be in place to control why, when and how subjects of access (specific individuals or software) areauthorized to have access to….	Subjects of access are not persons (individual) only. It is a software (process in computer) which have rights to modify, copy information also. For example, system process (software) should periodically copy confidential information (reservation copy). It works automatically and ithas rights to access to confidential information and copy this confidential information. It can copy information to forbidden directory and fail confidentiality.	X	Used "individuals and information assets are authorized" instead of adding a new term of subjects of access.		
14.	6.45	After an incident, the chronology of the	For the purpose of a detailed description of the	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		incident should be restored and its root causes identified. Lessons should be integrated into the regulated entity or competent authority's corrective actions. Such actions should include revising policies and procedures within the information security management system, enhancing information security measures, and augmenting training for personnel as needed to prevent future incidents.	information security incident management process				
NSGC — Pakistan/PAEC							
1	Para 1.10 (a)	The statement may be modified as follows: *"Establishing effective state legislative, **regulatory** and policy frameworks for maintaining the confidentiality, integrity and availability of sensitive information"*	Regulatory framework may be ensured regarding information security of sensitive assets.	X			
2	Para 1.11	The statement may be modified as follows: *".... outlining the particular provisions and conditions for those responsible for nuclear material, radioactive material, associated nuclear material, other radioactive material **and associated activities** in terms of information security."*	To complete the intent of the statement and achieve consistency with Para 1.13.	X	As this becomes repetitive with 1.12 reduced to: "outlining the particular provisions and conditions for information security within a nuclear security regime."		
3	Para 1.15	The statement may be modified as follows: *"The intended audience for this publication is all those who are responsible for the security of sensitive information, for example, competent authorities, including regulatory design and supply of nuclear bodies;*	Scope may be applicable to designers and vendors to complete the feedback process for improvement in design and supply of nuclear security related equipment; and also to conform to Para 2.14 (e).	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		management in facilities, companies or security related equipment. organizations involved in the use, storage or transport of nuclear material or other radioactive material; facility operators and personnel, ***designer, vendors,*** *and in particular security personnel; contractors or other third parties working for competent authorities, organizations or facility operators; or any other entities that have been given legitimate access to sensitive information."*					
4	Para 2.11	The statement may be modified as follows: *"Decisions made and actions taken by individuals, on the basis of information in whatever form, can have some significance for the functions performed relevant to nuclear security.* ~~*Information from sensors,*~~ *information objects containing procedures and set points, and information assets displaying this information will all contribute to decisions made by individuals."*	The term 'information objects' and 'information assets' covers the information from sensors and correspondingly the decision and actions to be taken by individuals, as evident from Figure 2.	X	Changed to raw signal information from sensors as it would be desirable to demonstrate a path through the Fig.		
5	Para 2.14	The following entities in bold may also be included in the list of entities: *i) Competent authorities,* ***regulatory authorities*** *with functions relevant to nuclear security;* ***Designer*** *of nuclear security system*	Regulatory authorities and designers of nuclear security and physical protection systems can also attribute value to information objects and information assets.	X			
6	Para 2.18	The statement may be modified as follows: *"The information necessary for the performance of a function important to safety, security or nuclear*	i) For conformance with para 6.22 b), information related to personal reliability programme may be included.	X	Suggest reliability and trustworthiness should be covered under safety/security. Safety function included now with alternate wording. Setpoints are also addressed but in		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		material accountancy and control, ***personal reliability and trustworthiness*** *can be considered as sensitive. Sensor values that are used to control nuclear reactivity,* ***essential safety function*** *for example, are ..... multiple sensors that serve different purposes. If the calibration table is manipulated or* ***set point values are modified****, multiple functions could be adversely affected, which means that both the sensor data,* ***verification of set point values****, of and the calibration table should be assessed as sensitive information."*	Essential safety function and set point values of system can be considered sensitive.		the concluding list of sensitive information to ensure a consistent example.		
7	Para 2.20	The following example may be included as sensitive information in nuclear safety and security: ***(h) Essential Equipment and System list***	Vital instrument to ensure safety and security functions may be included	X	Added "details of essential equipment and systems".		
8	Section 3	The title of the section may be modified as follows: Legislative, **Regulatory** and policy frameworks for securing sensitive information	For consistency.	X			
9	Para 3.1	The para 3.1 may be placed after para 3.2	Reference to Section 3 titled "Legislative and Policy Frameworks for securing sensitive information." The first para should list the available IAEA recommendations/guidance on the protection of the sensitive information and the 2nd para should supplement.	X	Both 3.1 and 3.2 were deleted following France Comment #6. Comment noted in case they are restored.		
10	Para 3.9	The statement may be modified as follows: *"The reporting of information security incidents to the competent authorities should be mandatory*	Regulations should describe the time frame in which to report the incident to ensure effective reporting.	X	Finished sentence with "within defined timeframes".		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		and laws or regulations should specify sanctions or penalties for failure to make such reports ***including timeframe in which to report the incident.****"*					
11	Para 3.11	The following may be included in the list of examples: (***g) Memorandum of Understanding, Non-Disclosure Agreements, Contracts and related instruments***	For completeness and to conform to paras 6.22b) and 6.25, for NDA and Contracts respectively.	X	As each of these items are organisation specific have modified for State-level agreements: (f) International instruments, such as conventions, on cybercrime (e.g. conventions, multilateral and bilateral agreements).		
12	Para 3.26	The statement may be modified as follows: *"The State's information security policy framework, or the more detailed nuclear security guidance, should identify clearly the regulated entities and competent authorities within the nuclear security regime that have delegated responsibility for* ***analyzing risks****, managing risks and defining rules for the protection of sensitive information…"*	To conform with Para 3.27 and Section 4.	X			
13	Para 4.4	Nuclear security event grading in Figure 4 may be removed.	Para 4.4 addresses scale of impact and information security requirements. The scope of the document covers information security for nuclear security.	X	This is just an example for illustrative purposes of how a nuclear security event grading could influence a classification decision. An alternate form of this diagram is published in NSS 42-G. Suggested for inclusion but prefix caption with "Example".		
NSGC — USA/NRC							
1.	6.40	Protecting the confidentiality, integrity, and availability of sensitive information from a potential cyberattack should be performed based on a graded approach.	The proposed guidance document does not address the use of a graded approach for cybersecurity.	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		Such a graded approach could be based on, for example, a consequence-based approach that relies on the severity of the potential consequences resulting from the compromise of the information following a cyberattack. The use of a consequence-based approach could allow facility operators to apply security measures to selected sensitive information objects and assets, with varying degrees of stringency.					
NSGC — Sweden/Swedish Radiation Safety Authority							
1	4.6/ 6	Specific consideration should be given to the accumulation ~~of information~~ and ~~points of concentration~~ aggregation of information	Aggregation is a more common word instead of "points of concentration".	X	Swapped concentration for aggregation but kept the accumulation as separate.		
2	4.6/end of para	(j) The need for classification within the classification scheme may change over time (k) Information that has not yet been classified should initially be managed using a conservative approach for the classification in order to prevent disclosure of information later proven to be sensitive.	Proposed additional factors.	X	Propose rewriting (j) to avoid ambiguity: The need for classifying certain information objects and information assets may change overtime as the understanding of threats and the consequences that could be realised evolve.		
3	1.5/5	modification, ~~alteration~~	The two words are synonymes.			X	Leaving to preserve the fact that this is a verbatim quote.
4	2.4/fig.1	The arrows ("Requires" and "Supports") on the right side of the figure should not be included in the figure	The information represented by these arrows is already included in the hierarchal structure of the rest of the figure.	X	Rather than remove the figures the caption has been edited to explain the basis for their inclusion, highlighting the need for effective governance structures to enable the right-most arrows.: "*FIG. 1. Relationship between the State's nuclear security objectives, information security governance structures and*		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
					the confidentiality, integrity and availability of information (adapted from Ref. [6]).“		
5	2.5/1	~~knowledge~~ information	Knowledge resides within a person.			X	This is an established consensus definition in a quote.
6	2.10/4	Information or data	The addition is necessary for consistency with the text in para 2.8	X	Removed data in 2.8		
7	2.12/6	Information or data	The addition is necessary for consistency with the text in para 2.8	X	Removed data in 2.8		
8	2.13/4	However, conventional	This restriction on the scope of what is regarded to be “information security measures” is a convention. There may be alternative interpretations for this expression.	X			
9	2.25/4 to end of para	~~However, the assessment…~~	The removed text is covered by the phrase “need to know”.	X	Accept that this is a detailed expansion but relocated the removed sentences to Section 5 at the point the concept in Section 2 is expanded on.		
NSGC — IEC SC45A							
1.	General	See specific proposed modifications in the following lines.	This document makes a few limited references to the use of standards. As a general rule, standards of course do not form part of a legislative framework and their application is not mandatory. This document does however recognize the use of standards as a means for formalizing contractual requirements between regulated entities and third parties for example (FIG 4). Additionally, and importantly, legislators do also often rely on standards as a means of demonstrating compliance with regulations, including in the field of information security/cybersecurity. In Europe, for example, these are referred to as harmonized standards which are quoted in the Official Journal of the European Union. Such standards may be developed internationally, at IEC level for example, and then adopted as European standards with or without modification in order to address specifically the European context. Similarly, standards can be adopted by states with or without modification which give them legal weight in those countries by which they may be used to demonstrate compliance	X	Addressed through 3.27: The competent authority for information security could designate national or international standards that may be adopted by regulated entities and competent authorities to demonstrate compliance with elements of the State’s information security policy framework and legislative framework. These standards may be used to guide the development of the regulated entities and competent authorities information security policy and information security management system.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			with national regulations. Standards are also sometimes developed by ISOs specifically upon the request of legislators in order to develop a consensual set of requirements to be applied by industry actors necessary for achieving compliance with regulations. Standards could therefore be extremely relevant and useful when developing a nuclear security regime.				
2.	Page 13: FIG 4.	Addition of International Standards Organisations into this figure. ISOs themselves would fall outside of "relevant entities" but harmonised standards could become part of the legislative framework.	See justification above.			X	The diagram explains the organisations that have a role in developing and implementing a State's nuclear security regime. It therefore reflects the national framework. Certifications and Standards are included in the figure. However, ISOs are outside of this State-level framework.
3.	3.5	I suggest rephrasing the following text: "*Competent authorities create the regulatory requirements for sensitive information.*" As follows: *"Competent authorities create the requirements necessary to achieve compliance with regulatory objectives regarding sensitive information. Such requirements could be based on the use of harmonized standards"*	See justification above. This proposal reflects the content of FIG 4.	X	As above addressed in 3.27		
4.	Page 13: Legislative and regulatory considerations	Addition of a paragraph explaining the above-described mechanism by which standards may become part of legislation (i.e. a means to achieve regulatory objectives) through harmonisation or through specific requests made by states to ISOs to develop new standards.	See justification above.			X	The role of standards as part of the national framework is already reflected in the text. Providing guidance to a State to request a standards body to develop a standard is not appropriate for the NSS.
5.	3.11	Addition of international or national/harmonised standards to this list of examples of potential sources to assist in defining and implementing nuclear security policies at is relates to nuclear security.	See justification above. This list is an informative list of examples and could therefore be extended to include non-legal aspects, especially for the *implementation* part. Implementing such security policies would typically require lower-level/industrially-applicable means, such as national or international standards which are based on consensus between all stakeholders.			X	3.11 lists legal instruments at the State level and international legally binding instruments that are part of the broader legal framework. .3.27 has been drafted to allow a CA to select a standard as a means of demonstrating adherence to regulation.

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
EPReSC — Indonesia/BAPETEN							
1.	4.2.	The competent authority for information security in relation to the nuclear security regime in each State should specify how to determine which information, relating to nuclear material, other radioactive material, and associated facilities and activities, constitutes sensitive information and how this information should be classified on the basis of the following criteria:	In some countries, for example Indonesia, competent authority for information security does not always address nuclear security	X	This is originally defined in 3.13 "(hereafter the 'competent authority for information security')". However recognise that the addition of "in each State" in 4.2 could add ambiguity and propose resolving by removing those words.		
2.	4.2. (b)	The usefulness of the information to a potential adversary seeking to compromise one or more nuclear safety and security functions.	Nuclear safety function can also be compromised by adversaries (for example computer systems that handle the performance of safety equipment)	X	"or" rather than "and"		
3.	5.8	The access of individuals to sensitive information should be controlled by a process or a procedure that grants access on the basis of the need to know principle and rescinds this access when this need no longer exists. The need to know principle could nevertheless be perceived as incompatible with the overall need to share information in order to support the performance of functions across a regulated entity or competent authority, provide resilience and allow for innovation. This incompatibility can be managed through an information security management system to anticipate and balance the risks to the nuclear security regime (see Section 6).	A process sometimes is written into a procedure	X			
4.	5.11.	Traditional information security measures are at times impractical for information whose sensitivity has a brief lifespan, for instance during the transport of nuclear material. In such cases, employing code words, gestures or signs can effectively reduce requirements for protection.	In the field, code gestures or signs can also be used for information protection	X	Added as *code words (including gestures or signs)*		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
5.	6.6.	An overall organization level information security policy should be developed and endorsed by management at the highest levels. It should include a statement of overall objectives, scope and importance. The policy is binding on all personnel, and therefore measures should be taken to inform personnel of their obligations in relation to the information security policy. Measures should also be taken to the personnel who have retired from positions holding sensitive information (for example, former head of security and former guards)	Personnel who are about to quit/retire will carry sensitive information in their next activities	X	Propose the following: "…obligations in relation to the information security policy, both during and after their term of employment as appropriate."		
6.	6.22. (b)	Personnel security, including trustworthiness determinations, should be used so that those who have access to sensitive information are deemed to be suitably trustworthy to a level established by the State in the information security policy framework. For information with a low classification, the regulated entity or competent authority should decide whether any determinations are necessary for personnel that need access; if deemed necessary, a limited check of an individual's background could be sufficient. For access to information with a higher classification, a more comprehensive set of background checks will be needed to determine trustworthiness. The personnel security process should also include the signing of a non-disclosure agreement between the member of personnel and the competent authority for information security or the respective regulated entity or competent authority. This agreement should also be signed by personnel who will be leaving or retiring from	Personnel who are about to quit/retire will carry sensitive information in their next activities	X	Propose adding this to the paragraph: …the respective regulated entity or competent authority, the obligations under such an agreement should be reinforced duration activities associated with the cessation of employment.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		positions involving sensitive information.					
7.	6.35.	The regulated entity or competent authority should also establish internal resources and a process to conduct internal inspections and audits. These inspections and audits should be performed to determine whether the practiced approach to information security complies with the regulated entity or competent authority's information security policy and whether it remains in compliance with the State's regulatory and policy frameworks. Through such inspections, the regulated entity or competent authority will be able to check compliance more frequently than they would in the case of having to undergo external inspections. Moreover, inspections or audits conducted by trained personnel who are familiar with the internal requirements, procedures and systems could identify opportunities for improvement that differ from those discovered through external inspection. In order to have trained personnel for internal inspections and audits, the regulated entity or competent authority may establish training and procedures for inspections and audits.	Good auditor/inspector can be obtained through training and procedures	X	Propose changing the last sentence as follows: Moreover, the regulated entity or competent authority may establish training and procedures for inspections and audits, to enable conduct by trained personnel who are familiar with the internal requirements, procedures and systems allowing the identification of opportunities for improvement that differ from those discovered through external inspection.		
8.	6.36.	External inspections are conducted by the competent authority for information security in relation to the nuclear security regime or other external organizations authorized to conduct inspection for information security. The aim of external inspections is primarily to assess the level of compliance with the State's regulatory and policy frameworks in an independent manner. When using external auditors, issues of confidentiality and	In some countries, for example Indonesia, competent authority for information security does not always address nuclear security. There is no clear law in Indonesia whether the competent authority for information security in Indonesia could conduct inspection in nuclear/radiation facility and associated facilities.	X	Noting 3.13 propose modification as follows: External inspections are conducted by the competent authority for information security or other external organizations authorized to conduct inspections for information security within the nuclear security regime.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		trustworthiness should be addressed in relation to the exchange of sensitive information with these external auditors.					
EPReSC — UAE/FANR							
1	3.22	The State should ensure that the information security policy framework defines interfaces between information security and all other relevant domains to ensure that all respective competent authorities are considered, as appropriate, including regulatory authorities, coordinating bodies or mechanisms, law enforcement, first responders, customs and border control, intelligence and security agencies, and health and environment agencies	Regulatory authorities (nuclear mainly) are key entities also in the framework of nuclear safety. The reference to first responders completes the paragraph in relation to additional key organizations responding to a security event that may trigger or potentially trigger an emergency situation; the reference to first responders also provides some link to the proposed new paragraph,	X	"Response organisations for nuclear or radiological emergencies" rather than first responders		
2	3.23	New Para: The State should ensure that the information security policy framework defines interfaces and is integrated as applicable with information needed for the response to nuclear or radiological emergencies.	IAEA standards on Emergency Preparedness and Response refer that the emergency response should be "executed and managed without impairing the performance of the continuing operational safety and security functions". Similarly, information security framework should not impair an effective response to emergency situations.	X	Proposed resolution achieved through comment #1.		
EPReSC — Australia/ARPANSA							
1	Where appropriate & References	Include security/safety interfaces if appropriate. This should include references to safety documents, including GSR2, EPR-METHOD and GSR7,	The scope states that "This Implementing Guide provides guidance on information security for nuclear security, and its interfaces with nuclear safety, and…" In this Step 7 draft there are zero references to Safety documents relating to interfaces. The DPP (see IAEA) states that "Interfaces with safety may include at least the	X	Added an EPR scenario to 9.3 in Annex II		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
			following IAEA publications:", and lists GSR2, EPR-METHOD and GSR7.				
EPReSC — Iran/ Environmental Protection, Radiation Emergency and Monitoring Department (EPREM)/ Iran Nuclear Regulatory Authority (INRA)							
1	1.7/ First line	"1.7. The terms used in this publication are to be understood as explained in the IAEA Nuclear Safety and Security Glossary…"	Editorial comment on complete title to The IAEA Glossary.	X			
2	2.6/ Bullet (b)	Clarification	This sentence is not so clear. Please revise it to be clear.	X			
3	3.1/ Last line	"… being taken or loss of availability of sensitive information could delay the response to an incident or emergency."	In case of an emergency, loss of availability of sensitive information could delay the response. So it is suggested to add "emergency".	X			
4	ANNEX I/ Paragraph I.6/Bullet (f)/ (iii)	"…the coordination and management of nuclear security measures, contingency operations and emergency response ~~plans~~ actions."	This bullet is about the effect of compromising communication channels or computer networks on management of some measures and operations like nuclear security measures. So it is suggested to change "emergency response plans" with "emergency response actions" with the following definition from IAEA Glossary: "**emergency response action**. An action to be taken in response to a nuclear or radiological emergency to mitigate the consequences of an emergency for human life, health, property and the environment."	X			
NUSSC — WNTI							
WNTI-01	Para. 1.16	(…). Section 3 describes the elements necessary to build a framework for the security of sensitive information within a State~~, and Sections 4–6 address each of these elements in turn~~. Section 4 presents considerations for determining which information can be considered sensitive information and would therefore need to be managed as such. Section 5	The text that it is proposed to delete is not clear and is useless. - Unclear, because it is not defined what are "these elements" that are mentioned here? Useless, because the next part of the paragraph clearly describes the contents of Sections 4, 5 and 6.	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		contains considerations for the sharing and disclosure of sensitive information. Section 6 describes the necessary actions at the regulated entity or competent authority for managing and operating measures to secure sensitive information. (…).					
WNTI-02	FIG. 5. Common scale of impact and a graded approach to protecting sensitive information (adapted from Ref. [6]).		Abbreviations such as "URC C", "URC B" and "URC A or HRC" should be defined.	X	Flag for editing but included in diagram as an example.		
WNTI-03	Para. 4.14	4.14. Some of the information in para. 4.~~14~~13 (e.g. personal information) could also be subject to specific security requirements under national laws not related to information security or could be subject to company policies.	Correction of typo. The relevant paragraph is 4.13.	X			
WNTI-04	FIG 6. A 'plan, do, check, act' cycle for the information security management system (adapted from Ref. [6]).		It should be clarified which "box" correspond to each step of the "plan, do check, act" cycle.	X	Swapped to continuous improvement cycle.		
WNTI-05	Table II-1 Category 1.5. Construction details Item A	Column "Rationale for sensitivity" ~~Official maps, charts or plans of sites could be released at the discretion of site management, provided they contain no description of the details of a building's functions, the material stored within the building, the location of internal security fences and other security measures employed at the building.~~ *An alternative text should be developed.*	The text does not fit with the purpose of the column "Rationale for sensitivity". The text should be reworded, or an alternative text be developed, to fit with the purpose of the column.	X			
WNTI-06	Table II-1	Column "Rationale for sensitivity"	The current text does not fit with the purpose of the column	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
	Category 1.7. Details of automated accesss control systems, (…)	~~Any details that could allow e~~**E**ither insiders or external adversaries to access and defeat such control systems are not to be released **might use any details to *(additional text to be developed)***.	"Rationale for sensitivity". In addition, the style is different from the other items. The text should be reworded, or an alternative text be developed, to fit with the purpose of the column.				
WNTI-07	Table II-1 Category 3.4. Transport packages: Information on the design of transport packages	Column "Sensitivity" ~~Confidentiality~~ **Not sensitive** Column "Rationale for sensitivity" **Information on the design of transport packages, without identification of construction details, is typically in the public domain. However, in some instances, ~~T~~**this **type of** information ~~can~~ **might** be useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport. **Consideration could be given to whether any of the information should be considered as "sensitive". Risk informed processes will help determine whether something is to be designated as "sensitive".**	The common practice is not to classify as "Not sensitive" the information on the design of transport packages.	X	Not sensitive/used the first sentence only to avoid ambiguity about sensitive or not in the example table.		
WNTI-08	Table II-1 Category 9.3. Exercises Item B	Column "Rationale for sensitivity" (…) the nature of tactics employed**.** Tampering with exercise details could lead (…).	Typo. A point is missing between "employed" and 'Tampering".	X			
WNTI-09	Table II-1 Category 12.2. Waste from decommissioning	Column "Category"	There is no footnote "b"	X			

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		12.2. Waste from decommissioning[b]					
NUSSC — Ukraine/SSTC NRS							
1. 2. 3.	First para of Scope Page 2 FIG. 3, Page 11 Para 3.21., Page16	This Implementing Guide provides guidance on information security for nuclear security, and its interfaces with other elements of a State's nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, and the detection of and response to nuclear security events. First box: e.g. Economic information, environmental information Second box: e.g. Business data, legislation and licensing information Third box: Security system information, material inventory information, personnel data Fourth box: e.g. Paper, magnetic, optical carriers of information, analogue crypto machines The State should ensure efficient functioning/performance of interfaces between information security and	In wording of the draft nuclear safety conjugates with elements of a State's nuclear security regime. That could lead to misunderstanding. Furthermore, in sequent sentence also the interfaces of information security for nuclear security with nuclear safety are mentioned, that could make a repetition. Military information is mostly secret information, strictly separated from other types of information in State, personally identifiable information belongs to a person as a rule. These examples are not especially suitable. Personnel data are sensitive information, as well as procurement data could be confidential. These may be included in third box. Plans, lists are information objects, as in Ref. [2]. Safes are not information assets, as do not contain, store or process the information. It is equipment for protection and secure storage of information assets, see 2.8 of the Draft and 3.3(g) in Ref. [1]. It is stated in 1.12 of the Draft document, that this	X	Scope reduced as recommender. A modification to Fig. 3 was performed combining other comments. Safes have been established as information assets by consensus in NSS 42-G and fit the definition in 2.8/2.9 (they perform an action). Merged in with other edits on 3.19/3.20/3.21.		

Comment No.	Para/Line No.	Proposed new text	Reason	Accepted	Accepted, but modified as follows	Rejected	Reason for modification/rejection
		other elements of a State's nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, as well as the detection of and response to nuclear security events. 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.	Guide provides guidance on interfaces of information security with other elements of a State's nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, as well as the detection of and response to nuclear security events. It will also address interfaces of information security with nuclear safety, nuclear material accounting and control and transport. Detailed recommendations are required based on the Ref. [3, 4, 5].				