Recommendations for the ongoing revision of IAEA NSS No 13 (INFCIRC/225 Rev 5)

Sarah Case Lackner, Ph.D.
Senior Fellow, Vienna Center for Disarmament and Non-Proliferation

NSS No 13 (INFCIRC 225) and the IAEA Nuclear Security Series

The International Atomic Energy Agency (IAEA) has been producing guidance on nuclear security, initially called the physical protection of nuclear material and facilities, for over 50 years. The first IAEA *Recommendations for the Physical Protection of Nuclear Material* were published in March 1972. In 1975, a revised and expanded version of these recommendations was published as INFCIRC/225[2]. It was revised again in 1977, 1989, 1993, 1999 and, most recently, in 2010. INFCIRC/225 in its current (fifth) revision[2] is considered by many governments and other entities to be authoritative on the subject of physical protection of nuclear material and facilities, and is referenced inter alia in some national regulations, in Project Supply Agreements and in numerous bilateral agreements.

For nearly thirty years, INFCIRC/225 was the primary publication from the IAEA on the subject of nuclear security. However, in 2006, the IAEA established the Nuclear Security Series (NSS). The NSS, currently standing at over 40 publications, includes four tiers of Member State consensus guidance, ranging from high level principles provided in the top tier publication, *Objective and Essential Elements of a State's Nuclear Security Regime* (NSS No 20) to specific, detailed technical guidance in the lowest-tier publications. The goal of the NSS is to form the basis of the Agency's work to support nuclear security around the world.

The most recent revision of INFCIRC/225, Revision 5, entitled *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)* was published in the Nuclear Security Series as NSS No 13 in 2010, as a Recommendations publication. This is one tier below NSS No 20 and at the same level as two other Recommendations publications: *Nuclear Security Recommendations on Radioactive Material and Associated Facilities* (NSS No 14) and *Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control* (NSS No 15). All four of

these publications, considered to be the "top tier" publications of the NSS, are used extensively by States and are interconnected with one another.

In 2019, the IAEA initiated a review of the top tier publications of the NSS, convening meetings of Member States to determine if there was a need to revise the publications in the coming years. In 2024, a decision was reached to undertake a revision of all these publications, including NSS No 13 (INFCIRC 225 Rev 5), with a focus on, among other topics, improving consistency across the top four publications, including in terminology, and ensuring that cyber security and new and emerging technologies are adequately represented in the guidance provided. Document Preparation Profiles (DPPs), as the IAEA refers to project proposals for publications, were approved for the concurrent revision of all four publications at the end of 2024 by the Member State body responsible for these matters, the Nuclear Security Guidance Committee (NSGC).

The first consultancy meetings involving Member State technical experts on the revision of these four publications, including on NSS No 13 (INFCIRC/225) took place at the beginning of 2025, and several have been held to date.

The audiences and primary uses of NSS No 13 (INFCIRC 225)

Unlike the other top tier publications in the NSS, which are of general interest to all States, NSS No 13 (INFCIRC 225/Rev 5) is of primary relevance to States with existing or planned nuclear programmes. As stated in paragraph 1.10 of the publication:

> *"The purpose of this publication is to provide guidance to States and their competent authority on how to develop or enhance, implement and maintain a physical protection regime for nuclear material and nuclear facilities, through the establishment or improvement of their capabilities to implement legislative and regulatory programmes to address the protection of nuclear material and nuclear facilities in order to reduce the risk of malicious acts involving that material or those facilities."*

The level of the publication is between the high-level essential elements for a nuclear security regime offered by NSS No 20, of use primarily to high-level decision makers, and the more detailed implementing guidance and technical advice provided by NSS No 27-G, *Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)* and NSS No 40-T, *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. However, NSS No 13 (INFCIRC/225 Rev 5) is generally perceived by Member States as more authoritative than the other NSS publications, as evidenced for instance by its inclusion in bilateral and trilateral agreements and, in some cases, national regulations.

NSS No 13 (INFCIRC 225/Rev 5) is primarily used by State competent authorities, such as the regulatory body, including as the basis for nuclear security regulations relevant to nuclear materials and facilities under civilian control. This is the reason it is often referred to as the "Implementing guide for the Amended Convention on the Physical Protection of Nuclear Material" (A/CPPNM).

The publication provides information on the objective and key elements of a State's physical protection regime (mirroring the Fundamental Principles of the A/CPPNM) as well as provides recommended requirements for consideration by national regulatory bodies for measures against:

- Unauthorized removal of nuclear material in use and storage,
- Sabotage of nuclear facilities and nuclear material in use and storage, and
- Unauthorized removal and sabotage of nuclear material during transport.

The publication does not specify the regulatory style to be used, whether prescriptive, performance based, or mixed, leaving this to national discretion.

Many national regulators indicate that their States "follow the spirit of NSS No 13 (INFCIRC 225/Rev 5) but do not necessarily follow it word for word, including in their implementation of their obligations under the CPPNM/A. This is particularly common among more advanced nuclear States, ´who may follow a partly or primarily performance-based approach to regulation.

The recommendations provided in NSS No 13 (INFCIRC/225) are not binding on IAEA Member States, particularly as nuclear security is considered a State responsibility.

Why is a revision needed to NSS No 13 (INFCIRC/225)?

NSS No 13 (INFCIRC/225 Rev 5) was published in 2011, now more than 14 years ago. Over the last 14 years, there have been a number of international shifts with implications for the security of civilian nuclear materials and facilities, among them:

- Major international events with implications for nuclear security, such as the 2014 event at Fukushima Daiichi in Japan (due in part to failures in safety culture) and the potential targeting of civilian nuclear infrastructure in the ongoing war in Ukraine;
- The recognition of an increasing need for resilience in nuclear security measures following the COVID-19 pandemic;
- The integration of digital devices and, in particular, interconnected devices into nearly every facet of life;
- Increasing digitalization of all industrial sectors, including the nuclear sector;

- The rise of new and emerging technologies such as artificial intelligence systems and models, additive manufacturing, quantum encryption, advances in drone technologies, and more.

In light of this, it is essential to ensure that the recommendations provided for States in NSS No 13 (INFCIRC/225 Rev 5) continue to reflect the best practices to ensure the security of nuclear materials and nuclear facilities in the modern world. In addition, a further topic that should be addressed in the revision involves ensuring consistency across the top tier of the NSS publications. While this paper focuses on NSS No 13 (INFCIRC/225 Rev 5), it is important for the usability of all four top tier publications by States to ensure that they are consistent with one another and do not introduce any unintended conflicts that could be misinterpreted by a newcomer State.

Potential improvements to NSS No 13 (INFCIRC/225 Rev 5) in this revision

The DPP for the revision of NSS No 13 (INFCIRC/225 Rev 5) highlights a few gaps to be addressed by the revision, including revising of unclear and inconsistent definitions, ensuring consistency of terminology and concepts among the top tier publications, and enhancing the text to address specific areas, such as information and computer security, insider threats, emerging threats, new and emerging technologies to strengthen nuclear security, safety-security interfaces, security aspects of nuclear material accounting and control (NMAC) and sustainability and resilience of nuclear security regimes in unplanned situations. These changes, as set out in the DPP, are relatively modest, and the limited nature of the revision is repeatedly underscored.

However, it has been suggested by others that more extensive updates to NSS No 13 (INFCIRC/225 Rev 5) would be valuable. For example, Bunn et al[3] suggested that, based on the results of the 2010, 2012, 2014 and 2016 Head of State-level Nuclear Security Summits as well as the INFCIRCs published by the IAEA and endorsed by a number of States after, that there are significant areas of improvement that could be incorporated in a revision to NSS No 13 (INFCIRC/225 Rev 5).

This report advocates for a revision that updates and clarifies the publication, but does not introduce dramatic changes. There is value in focusing on the most important forward-leaning concepts , including because a limited set of changes will then be able to be adopted more rapidly than if a large number of changes were introduced. While there are improvements to be made, the long-term stability of the publication is of key importance to ensure its continued relevance. While there are agreements in which “all future revisions of INFCIRC/225” are required to be followed, there are many others that refer to a specific revision, or simply rely on its principles when drafting regulations and legislation. In these latter cases, simply revising an

IAEA publication will not necessarily result in a sudden shift in understanding of the scope and details of international nuclear security, but the lag time is likely to be proportional to the ambition of the change, potentially overlapping with even the next revision. Further, any change will need to be agreed to by all Member States, a complicated proposition.

In the remainder of this paper, concrete recommendations for improving and strengthening NSS No 13 (INFCIRC/225 Rev 5) will be set out for discussion and consideration, including examples of how these recommendations could be realized in a revision of the publication.

NSS No 13 is best seen as a single piece in a larger framework of guidance provided by the IAEA on this topic. This is a valuable approach, as it keeps the individual publications focused and readable. In addition, details that are specific to how States implement a physical protection regime are better handled in lower level publications As these are more frequently updated, this ensures that the latest developments can be included. On the other hand, evergreen and holistic topics may be better handled at a higher level, in the NSS Fundamentals, which change even less frequently than the recommendations.

Recommendations

In the following section, a few key areas in which NSS No 13 (INFCIRC/225 Rev 5) could be improved are highlighted, specifically: cyber and data security; emerging threats and emerging technologies; sustainability, flexibility and resilience; insider threats; nuclear security culture; and advisory missions and international cooperation. While these are priority areas, this is not an exhaustive list, and additional areas of potential improvement are certain to be identified by IAEA Member States during the revision process.

Some specific suggestions of textual revisions that might be made are suggested in the sections to follow, but as with the areas of potential improvement, there are many ways that these suggestions could be implemented, and these suggestions are only intended to spark discussion.

Cyber and data security

A top priority for the revision of NSS No 13 (INFCIRC/225 Rev 5) should be to ensure that the role of cyber security in physical protection of nuclear material, facilities and activities is adequately addressed. In 2011, the importance of cyber and data security was growing rapidly but nowhere near the level of importance it has reached today. With the advent of sophisticated artificial intelligence (AI) models and systems that can rapidly process open-source information

and write computer code or text that could assist an attacker, security of sensitive information as well as security of computer systems will only increase in importance in the coming decade.

In the NSS generally, "computer security" is used to mean what is elsewhere referred to as "cyber security".[4] [5]In NSS No 13, even the term "computer security" is not used, although in two places (4.10 and 5.19), "cyber attack" is mentioned. This should be remediated, and reference to computer security should be made throughout the text.
Computer security is best addressed via changes throughout the text to highlight its role in physical protection, rather than through the addition of a dedicated section. This approach not only preserves the overall structure of the publication, but also recognizes how embedded digital systems are in the modern world, including in nuclear facilities and activities. A separate section would, while emphasizing the importance of computer security, also give the impression that computer security is an "extra" that might be avoidable. In the modern world, given the extensive use of digital systems on the business side (including for sensitive data), as well as increasingly in operational technology, this is unrealistic.

Some suggestions follow:

- Given the increasing importance of data security and information protection, a paragraph on providing for the establishment of regulations and requirements for computer, data and information security should be added under the text on Fundamental Principle G: Legislative and Regulatory Framework (paras 3.9 – 3.17). This would strengthen the relevance and position of lower level publications describing this in more detail. For example:
    - 3.10 (add at end) *These requirements should include those for the security of computer systems, networks and data associated directly or indirectly with the physical protection of nuclear material in use, storage and during transport, and for nuclear facilities, using a graded approach.*
- In or directly after paragraph 3.28, which addresses security by design, it would be useful to note that computer security by design, taking a systems view across the entire facility, is needed, particularly given the trend towards increasing digitization in all parts of nuclear facilities. For example:
    - 3.28 (add at end): *Further, cyber security should be taken into account when designing the facility, using a systems approach and including any networked devices and other digital systems planned for use in the facility.*
- In paragraph 3.42, which addresses managing risk, computer and data security measures should be explicitly called out. For example:
    - Risk can be managed by:
        - (new bullet) *Improving the effectiveness of computer and data security. Ensuring that malicious actors are not able to access or manipulate computer systems used in nuclear facilities and that confidential data,*

including digital data, remains confidential, will increase the difficulty of organizing an effective attack on material or a facility.

- Where confidentiality is discussed, at a minimum, specific examples highlighting digital/computer data and information security should be added as appropriate, to provide hooks for text provided in lower level publications. Security-relevant data are not just sensitive information on security procedures, but will grow to include a need to protect a range of data relevant to facility operations, including that collected via electronic means (e.g., that collected by internet of things devices) or stored in the cloud (remotely).
- At the start of the recommended requirements sections or elsewhere early in the draft, the increasing tendency towards automation and use of digital systems in facilities and activities should be mentioned, noting the need to ensure the security of such systems as well as the data associated with them. Paragraph 4.10 and 5.19 mention computer-based systems, but are too limited in their scope (physical protection, nuclear safety and NMAC), which does not cover the full scope of possible digital applications in operational technology or on the business side. This text could be replaced with something along the lines of:
    - 4.10 (alt) and 5.19 (alt) *Digitised systems used in facilities as well as those accessing sensitive digital data related to nuclear facilities should be protected against compromise (e.g. cyber attack, manipulation or falsification), consistent with the Design Basis Threat.*

These are simply a few examples of where text could be added to highlight the many ways in which cyber security is becoming an indispensable part of nuclear security. In a thorough revision, these types of suggestions should be supplemented by a close review of the text in chapters 4, 5 and 6 to ensure that additional references are added as needed.

Emerging threats and emerging technologies

Specific examples of emerging threats should only be inserted into the text of NSS No 13 (INFCIRC/225 Rev 5) when it is unavoidable, for example, to explain a need for a change to principles of physical protection. The current rapid technological pace of change means that it is impossible to predict which technologies are likely to be of most concern or benefit with respect to physical protection in 5-10 years, and the new revision needs to realistically be applicable for a minimum of 10 years.

An emphasis on flexibility with respect to emerging threats is highly advisable, alongside minimal, broad language. Further, detailed information can be provided in lower-level guidance and in informational publications that have a shorter intended life cycle. Possible edits to text include the following (suggested edits in italic):

- Paragraph 3.2 could be edited to maintain flexibility while mentioning emerging threats: " The State's physical protection regime should be reviewed and updated regularly to reflect changes in the threat**,** *including those due to new and emerging technologies*…"
- Paragraph 3.39 could be edited as well, by adding "evaluate the implications of any changes in the threat assessment or design basis threat, *with particular attention to those changes due to new and emerging technologies*".
- Paragraph 3.40, which currently focuses on airborne and stand-off threats, could underscore this issue and be broadened to "… against possible stand-off attacks **or** *those involving new and emerging technologies, digital and otherwise*, as specified in the State's threat assessment or DBT."[6]

Further on in the text, a brief reference to the importance of encrypting communications and considering the implications of misinformation in emergency response could be helpful.

With respect to new technologies that could be used to strengthen security, the need to ensure that these technologies are carefully considered could be highlighted by adding text early in the publication with reference to ensuring the regime is updated, for example, by adding a clause (italic) to 3.2 such as:

- 3.2: The State's physical protection regime should be … updated regularly to reflect changes in the threat and advances made in physical protection approaches, systems and technology, *including new and emerging technologies that could be used to strengthen physical protection systems***…"**

To complement this reference, in each of the General sections for chapters 4, 5 and 6, which set out the recommended requirements, a sentence or paragraph might be added to note the importance of such technologies. For example, text could be:

- *Operators should consider use of emerging technologies as appropriate to improve security systems as well as to strengthen cyber security capabilities.*

Sustainability, flexibility and resilience

The worldwide COVID-19 pandemic underscored the importance of preparing for the unexpected, and these lessons should be clearly incorporated in the revision of NSS No 13 (INFCIRC/225 Rev 5). Doing so effectively would not require extensive changes to the text, but could be accommodated with relatively simple adjustments to underline the importance of the concept.

For example, an addition to paragraph 3.56 could be made:

- 3.56 The State should establish a ~~sustainability~~ programme to ensure that its physical protection regime is sustainable and effective in the long term **as well** *as resilient, including in unplanned situations for which continuity of operations is needed. This*

includes ensuring the regime is sufficiently robust to such unplanned situations and committing the necessary resources for both sustainability and resilience."

Insider threats

Insider threats are clearly addressed throughout the text of NSS No.13 and are explicitly called out in paragraph 3.36 as threats to be protected against. The placement of this reference under the identification and assessment of threats is logical, but it could be significantly expanded on, to draw attention to the topic in light of the growing concern in this area, given the potential for increasingly sophisticated social engineering attacks aided by AI systems. This reference could be strengthened.

As noted by Bunn et al, INFCIRC/908/Rev 1 provides some useful suggestions in this arena. Drawing on key points made in this INFCIRC, a new paragraph to follow para 3.36 could be generated, for example:

3.36bis: States should develop and implement a training programme to mitigate insider risk, implement robust trustworthiness programmes, strengthen nuclear security culture and ensure that defined physical protection design objectives and/or measures are put in place with respect to insiders. In addition, due attention should be paid to the potential for recruitment of insiders via social engineering techniques and the potential for cyber insiders.

This text could be strengthened by connecting it to high level text inserted into NSS No 20, to recommend a national level insider threat mitigation policy.

Further, on a more detailed note, no mention is made of insider threats with respect to transport in chapter 6, although this could be a significant threat, including if sensitive information on transports is provided to an outsider. This could be a useful improvement, for example, adding a bullet to paragraph 6.6 to address this topic, along these lines:

- 6.6 (j) (new)*Minimizing the opportunity for an insider to divert nuclear material or provide sensitive information regarding the conveyance to outsiders.*

Nuclear security culture

While nuclear security culture is stressed in NSS No 13 (INFCIRC 225/Rev 5), it has become increasingly important over the last decade and strengthening reference to it in the publication would be valuable. This strengthening could build on the existing section on nuclear security culture, paragraphs 3.48 – 3.51. Two potential sentences that could be helpful are in italics below, to add to the existing paragraphs

- **3.50:** The State should promote a nuclear security culture and encourage all security organizations to establish and maintain one. A nuclear security culture should be pervasive in all elements of the physical protection regime. *The importance of this culture should be promoted from the very top management of organizations, as an essential part of an overall organization culture.*

- **3.51** All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection. *These organizations should also undertake regular self-assessments of nuclear security culture.*

Another possible addition could be to focus on the importance of cyber security in the modern world as part of a nuclear security culture, as well as attention to the links between new and emerging technologies and nuclear security culture:

- (new) 3.51bis *Nuclear security culture in the organization should include due attention to cyber security, as well as account for novel challenges at the interface between nuclear security culture and new and emerging technologies.*

Advisory missions and international cooperation.

While there is a dedicated section in international cooperation and assistance in NSS No 13 (INFCIRC/225 Rev 5), there is no mention of the importance of advisory missions. The IAEA's International Physical Protection Advisory Service (IPPAS) conducted its first meeting in 1996, and conducted its 100th in 2023. These missions are broadly recognized as being of significant value for Member States, and it would be worthwhile to highlight this in the recommendations. For example, a new paragraph could be added:

- 3.31bis *International advisory missions, such as those provided by the IAEA, can provide helpful feedback for States on potential improvements to their physical protection regime.*

Conclusion

In making these recommendations for potential improvements and updates, there are challenges inherent in the fact that any changes to the text of NSS No 13 (INFCIRC/225 Rev 5) need to gain consensus with all Member States. In many cases, Member States will have valid disagreements regarding the necessity or validity of certain changes. Further, the value of stability of the publication will need to be factored in. However, at the same time, a lack of change over time will result in a publication that is no longer useful and thus no longer used. Given the essential role of this publication in ensuring a high, consistent standard of nuclear security internationally, this would be a significant – and potentially dangerous – loss.

NSS No 13 (INFCIRC/225 Rev 5) has only been revised an average of every 10 yearssince its inception. The current ongoing revision provides a significant opportunity for Member States to bring this publication up to date with the many changes that have occurred since 2011. This will preserve its value for States in the coming decade, and it is worthwhile for States to make significant efforts in this direction.

[1] The most recent revision of NSS No 13 (INFCIRC 225 Rev 15) can be found on the IAEA website at: https://www.iaea.org/publications/8629/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities-infcirc225revision-5

[2] Information circulars are published from time to time under the symbol INFCIRC/... for the purpose of bringing matters of general interest to the attention of all Members of the Agency. (INFCIRC/1 Rev 14)

[3]IAEA Nuclear Security Recommendations (INFCIRC/225): The Next Generation

[4] While not strictly necessary, a footnote could help to clarify the use of the term computer security, and that it is used to refer to what is elsewhere called cyber security.

[5] It could also be useful to clarify the relationship of information and computer security to “physical protection”. Footnote 1 in NSS No 13 establishes an equivalency between “physical protection” and “nuclear security of nuclear materials and nuclear facilities”, however, typically computer security is considered to be an add-on to physical protection, rather than encompassed in it. It would be useful for the relationship to be made clear, as this will affect the interpretation of whether computer security needs to be taken into account as appropriate in each mention of physical protection throughout the text.

[7] This would also eliminate the apparent „stuck in the past” nature of thinking primarily about airborne attacks.