Chapter 8

The Efficacy of the Global Nuclear Security Legal Regime and States' Implementation Capacity in Light of the Forthcoming Development of Advanced Nuclear Reactor Technologies

Bonnie Denise Jenkins

Contents

8.1	Introduction	162
8.2	Reviewing the Primary International Components of the Global Nuclear Security Legal Regime	163
8.2.1	The Convention on the Physical Protection of Nuclear Material and Its Amendment	163
8.2.2	INFCIRC/225/Rev.5	164
8.2.3	IAEA Nuclear Security Series	166
8.2.4	Cybersecurity	167
8.3	Reviewing the Ability of States to Implement any New Nuclear Security-Related Requirements or Guidance	168
8.3.1	Role of Supplier States and Suppliers	168
8.3.2	Role of the IAEA	169
8.4	Conclusion	170
	References	170

Abstract The forthcoming arrival of small modular reactors and other advanced nuclear reactor technologies can be an immensely beneficial development in the world's collective pursuit of energy security and meeting climate change objectives. The key question is whether or not these new reactor technologies significantly alter the fundamental premises underlying the existing nuclear security legal regime. The Convention on the Physical Protection of Nuclear Material and its Amendment (A/CPPNM) are the only legally binding international instruments governing the physical protection of nuclear materials and nuclear facilities. Together the A/CPPNM and the international guidance on nuclear security comprise the current legal framework for nuclear security. This chapter examines whether the A/CPPNM

B. D. Jenkins (✉)
US Department of State, Washington, DC, USA
e-mail: Official.Mail@iaea.org

adequately covers advanced reactor technologies; and whether the States that are interested in acquiring these new reactor technologies have the capacity to effectively implement the associated legal requirements, regulatory standards, and international guidance that comes along with such technologies. The analysis touches upon the role of the International Atomic Energy Agency (IAEA), the IAEA Nuclear Security Guidance, and issues of cybersecurity.

Keywords Convention on the Physical Protection of Nuclear Material (CPPNM) · The Amendment to the Convention on the Physical Protection of Nuclear Material · Physical protection · Small modular reactors (SMRs) · Advanced nuclear reactor technologies · Cybersecurity · IAEA nuclear security series · Supplier states · Suppliers

8.1 Introduction

As the use of nuclear energy became more widespread in the 1960s and 1970s, the international community became increasingly aware of the need for a shared set of practices to ensure the appropriate physical security of nuclear material under civilian use. At the time, light water reactor technology was the only widely commercialized type of civilian reactor and the international community's efforts to develop nuclear security-related agreements, regulations and guidance were consequently developed with it in mind. Looking into the future, it appears likely that over the next few decades the dominance of light water reactors will fade and give way to advanced reactor technologies, including small modular reactors (SMRs). With this in mind, practitioners responsible for the long term effectiveness of the global nuclear security legal regime are compelled to question if the existing regime will need to be updated. The key question is whether or not these new reactor technologies significantly alter the fundamental premises underlying the existing nuclear security legal regime. Is the scope of the relevant international convention, the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment (A/CPPNM),¹ sufficiently broad to ensure their provisions apply to advanced reactor technologies? Is other relevant international guidance sufficiently broad? Will States that are interested in acquiring these new reactor technologies have the capacity to effectively implement the associated legal requirements, regulatory standards and international guidance that come along with such technologies?

In order to review these questions, we must first examine the A/CPPNM and associated international guidance which together establish our current legal framework. The second key question relates to the ability of States to undertake their primary responsibility for physical security of nuclear material and nuclear facilities under their jurisdiction once these new reactor technologies become a reality. In the end, we

¹Convention on the Physical Protection of Nuclear Material, opened for signature 3 March 1980, entered into force 8 February 1987 (CPPNM); Amendment to the CPPNM, entered into force 8 May 2016 (A/CPPNM).

believe that there does not need to be widespread revision of the current nuclear security legal regime and related guidance to account for newly emerging civil nuclear reactor technologies and wish to lay out the basis behind that conclusion.

8.2 Reviewing the Primary International Components of the Global Nuclear Security Legal Regime

8.2.1 The Convention on the Physical Protection of Nuclear Material and Its Amendment

In recognition of the growing need for a common set of international standards defining adequate physical security for the international transport of nuclear material, the CPPNM was opened for signature on 3 March 1980, and entered into force on 8 February 1987. By the late 1990s, and particularly subsequent to the events of 11 September 2001, a large number of States maintaining nuclear material recognized the need to expand the scope of the CPPNM to include the physical protection of nuclear material in domestic use, storage and transport, and the protection of nuclear materials and facilities against sabotage. Consequently, States Parties to the CPPNM adopted by consensus an Amendment to the Convention on 8 July 2005, which entered into force on 8 May 2016, in accordance with Article 20.2 of the Convention. The CPPNM and its Amendment together comprise the only legally binding international convention governing the physical protection of nuclear materials and nuclear facilities. In the context of advanced nuclear reactor technologies, it is vital to note that unlike the CPPNM, the A/CPPNM includes nuclear facilities within its scope.

When considering the question of whether the A/CPPNM adequately covers advanced reactor technologies, we must examine Articles 1, 2, and 2A, which relate to its scope. Article 1(d) defines “nuclear facility”, for purposes of the A/CPPNM, as “a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material”.² Article 2 states that the Convention “shall apply to nuclear material used for peaceful purposes in use, storage and transport and to nuclear facilities used for peaceful purposes”.³ Article 2A requires that each State Party shall “establish, implement and maintain an appropriate physical protection regime applicable to nuclear material and nuclear facilities under its jurisdiction with the aim of: (a) protecting against theft and other unlawful taking of nuclear material in use, storage and transport;... [and] (b) protecting nuclear material and

²A/CPPNM, above n.1.

³A/CPPNM, above n.1.

nuclear facilities against sabotage”.⁴ Article 2A(3) also requires each State Party to apply a set of Fundamental Principles of Physical Protection of Nuclear Material and Nuclear Facilities.

Several of these Fundamental Principles relate to the nature of the nuclear facility in question. Fundamental Principle F (Security Culture) provides that “[a]ll organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.”⁵ Fundamental Principle G (Threat) provides that a State’s physical protection “should be based on the State’s current evaluation of the threat.”⁶ Fundamental Principle H (Graded Approach) states, in part, that physical protection requirements “should be based on a graded approach, taking into account the current evaluation of the threat ... and potential consequences associated with ... sabotage against ... nuclear facilities.”⁷ Fundamental Principle I (Defence in Depth) provides that a State’s physical protection “should reflect a concept of several layers and methods of protection ... that have to be overcome or circumvented by an adversary in order to achieve his objectives.”⁸

With these requirements identified, we must turn to examining if any of them suggest changes are in order in light of forthcoming advanced reactor designs. The definition of “nuclear facility” in Article 1 of the A/CPPNM does not specify any type of nuclear technology or the nature of the operation of the reactor. The requirements of Article 2 do not impose any such limits either. Article 2A’s specific requirements related to theft, unlawful taking and sabotage similarly do not limit the scope of their applicability based on the type of facility or reactor technology in any way. Fundamental Principles F, G, H and I therefore all contain sufficiently inclusive language so as to obviate the need to amend them for the purpose of capturing these new technologies.

Accordingly, no amendments to the A/CPPNM would be required to adequately cover future advanced reactor technologies within its scope.

8.2.2 *INFCIRC/225/Rev.5*

In 1975, the IAEA Director General convened a group of experts to review a draft booklet of recommendations for IAEA Member States for the physical protection of nuclear material.⁹ These recommendations were subsequently updated and brought to the attention of IAEA Member States in the form of INFCIRC/225¹⁰ published

⁴ A/CPPNM, above n.1.

⁵ A/CPPNM, above n.1.

⁶ A/CPPNM, above n.1.

⁷ A/CPPNM, above n.1.

⁸ A/CPPNM, above n.1.

⁹ IAEA 1975.

¹⁰ Ibid.

in September 1975. In the ensuing years, INFCIRC/225 has been significantly updated and expanded in scope. The current version is published as Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5)¹¹ and was released in January 2011. INFCIRC/225/Rev.5 reflects the IAEA's most thorough and comprehensive set of recommendations on the physical protection of nuclear material and nuclear facilities. It is an important step forward as it provides guidance for the first time on a number of new issues, including protecting digital systems used for physical protection, nuclear safety, and nuclear material accountancy and control against a cyberattack.¹² Revision 5 also references concern about insider threats and stresses the importance of developing an appropriate security culture within a State's nuclear programme.¹³

While Sections 1 and 2 are introductory in nature, Section 3 of INFCIRC/225/Rev.5 lists the elements of a State's physical protection regime for nuclear material and nuclear facilities and corresponds to the Fundamental Principles in the A/CPPNM. How these elements are applied will depend on what type of nuclear facility is in question. Section 3 recommends the creation of a threat assessment and, if appropriate, a design basis threat. It recommends that physical protection requirements should be based on a graded approach taking into account the nature of the nuclear material, and the potential consequences associated with the unauthorized removal of material and with the sabotage of the nuclear material or facility.¹⁴ The section recommends that physical protection reflect a concept of several layers of protection that have to be overcome by an adversary,¹⁵ and stresses the need to prioritize the development and maintenance of a security culture.¹⁶

Section 4 of INFCIRC/225/Rev.5 reviews in greater detail requirements for measures against unauthorized removal of nuclear material in use and from storage. Section 4.9 recommends that the physical protection system of a nuclear facility should be integrated and effective against both sabotage and unauthorized removal.¹⁷ Sections 4.13–4.49 list specific physical security recommendations for facilities holding Category I material, but the recommendations do not have applicability to any specific reactor technology. Section 5 lists specific requirements for measures against sabotage of nuclear facilities and nuclear material in use or storage. It highlights a number of different ways in which the physical protection system of a facility can be designed in order to mitigate the risks of sabotage.¹⁸ The section also highlights a number of spatially related issues (e.g. establishment of specifically defined

¹¹IAEA 2011.

¹²Bunn et al. 2020.

¹³Ibid.

¹⁴IAEA 2011.

¹⁵Ibid.

¹⁶Ibid.

¹⁷Ibid.

¹⁸Ibid.

and distinct areas, vehicle barriers installed at an appropriate distance from vital areas) but none that are limited to any specific reactor technology.¹⁹

In sum, a detailed review of the specific provisions of Sections 3–5 of INFCIRC/225/Rev.5 reveals that while there are many recommendations that pertain to the construction and operation of a nuclear facility, none of its provisions are specific to the type of nuclear facility. Accordingly, it is not foreseen that any changes will need to be made to INFCIRC/225/Rev.5 for the specific purpose of capturing advanced reactor designs.

8.2.3 IAEA Nuclear Security Series

In March 2002, the IAEA Board of Governors approved the Agency’s first “Nuclear Security Plan (for 2002–2005).”²⁰ The Plan included the development of “standards, guidelines, and recommendations” across the broadened scope of the Agency’s nuclear security activities as approved by the Board.²¹ That same year, the IAEA Director General established a group of experts to provide advice on the content and priorities of the IAEA’s nuclear security activities—the IAEA Advisory Committee on Nuclear Security (AdSec). Upon the Board’s adoption of the Plan, AdSec became immediately involved in the development of such standards, guidelines and recommendations.²² With AdSec’s recommendation, the IAEA Publications Committee approved the establishment of the Nuclear Security Series in 2004.²³ From 2006 onward, IAEA Nuclear Security Series publications have been issued in the following four categories:

- Nuclear Security Fundamentals to contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations;
- Recommendations to present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals;
- Implementing Guides to provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation;
- Technical Guidance publications to include: Reference Manuals, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; Training Guides, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and Service Guides, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.²⁴

¹⁹IAEA 2011, paras 5.25–5.31.

²⁰IAEA Nuclear Security Guidance Committee (NSGC)—Chairman’s Report of the NSGC’s First 3-Year Term (2012–2014), p. 6.

²¹Ibid.

²²Ibid.

²³Ibid.

²⁴Ibid.

Both the Nuclear Security Fundamentals and Recommendations documents are written at high levels and consequently, neither the Fundamentals nor any of the Recommendations documents are sufficiently detailed to be reactor design-specific in any way. The Implementing Guides and the Technical Guidance are more detailed in nature, and accordingly, it is appropriate to examine a few of the most likely documents to contain such language.

Nuclear Security Series (NSS) Implementing Guide No. 8-G (Rev. 1) entitled Preventive and Protective Measures Against Inside Threats discusses specific protective measures related to detection, delay, response and emergency plans but there are no reactor technology-specific provisions.²⁵ NSS Implementing Guide No. 10-G (Rev. 1) entitled National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements provides guidance on conducting threat assessments and developing and maintaining a design basis threat for a specific facility but it does not include any reactor technology-specific recommendations.²⁶ NSS Implementing Guide No. 27-G entitled Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) is the lead Implementing Guide in a suite of guidance to States on implementing the recommendations of INFCIRC/225/Rev.5. However, it too does not reach the level of specificity where reactor technology-dependent language is utilized. Accordingly, as with the A/CPPNM and INFCIRC/225/Rev.5, all existing provisions in the NSS guidance are sufficiently inclusive to capture advanced nuclear reactor technologies.

Taken as a whole, the international community's existing set of legally binding agreements and guidance is sufficiently broad to account for the advent of advanced nuclear technologies. That said, complexities may arise in how individual States implement the aforementioned requirements and guidance in a way that effectively meets the specific nuclear security challenges and risks in their territory. As States construct and operate these new reactors, lessons will be learned and updated or additional IAEA guidance at the Implementing Guide and/or Technical Guidance level may prove useful.

8.2.4 *Cybersecurity*

Beyond the specific Convention and related guidance described earlier, there is one unique subject that merits particular consideration: cybersecurity. At this time, all advanced nuclear reactor designs are forecasted to include digital automation as an integral component of their operations. As a consequence of this automation, the risks of a cybersecurity-related incident increase. The IAEA has previously published several relevant Implementing Guides and Technical Guidance (which refers to cybersecurity as computer security) that bear directly and/or indirectly on

²⁵IAEA 2020.

²⁶IAEA 2009.

developing mitigation techniques to thwart cybersecurity risks. The existing Implementing Guides and Technical Guidance are written broadly enough to apply to advanced reactor technologies, but as these new technologies become available online, the IAEA and its Member States should consider the benefits of developing additional specific Implementing Guides or Technical Guidance on the specific cybersecurity-related challenges to the physical security of advanced reactor designs.

8.3 Reviewing the Ability of States to Implement any New Nuclear Security-Related Requirements or Guidance

In addition to considering the adequacy of international legal requirements and recommendations related to nuclear security to cover advanced reactor designs, the second key question is whether States interested in acquiring these new technologies will have the capacity to effectively implement the associated legal requirements, regulatory standards, and complementary guidance that comes with such technologies. As the responsibility for the establishment, implementation and maintenance of a physical protection regime rests entirely with the State, if it lacks such a capacity, what are some ways to assist States to acquire it? While the global nuclear security legal regime is sound, there is a continuing need to strengthen domestic legal and regulatory frameworks.

8.3.1 Role of Supplier States and Suppliers

In the design and construction of new reactor technologies, both supplier States (through their licensing authorities) and suppliers must be mindful of all elements of an adequate nuclear security system, including security culture, threat (including the development of an appropriate design basis threat), a graded approach, and defence in depth principles as discussed earlier. As representatives of governments, licensing authorities carry the ultimate responsibility for ensuring that the supply of these reactors occurs in accordance with the highest global standards of safety, security and non-proliferation. Accordingly, licensing authorities have a heightened and specific duty to ensure that physical security considerations specific to these new technologies are factored into their decision making process. They should proactively assert to suppliers the importance of incorporating security culture, threat, graded approach and defence in depth principles into their reactor designs. Similarly, suppliers should be encouraged to consult with their licensing authorities early on to ensure that reactor designs are consistent with international legal requirements and guidance.

The United States of America (USA) takes these responsibilities very seriously and has been preparing for the nuclear security-related implications of advanced reactor technologies for many years. The US Nuclear Regulatory Commission (NRC)

has been focused on the licensing impacts of these technologies and has created a number of internal working groups to study their implications and its ability to license them in a comprehensive and timely manner. In 2019, the NRC identified the need to amend its regulations to develop more specific physical security requirements for advanced reactors. This action was designed to provide a “clear set of performance-based requirements and guidance for advanced reactor physical security” as well as “establish greater regulatory stability, predictability, and clarity” for advance reactor licence applicants.²⁷

Working with NRC, the US nuclear industry also engaged as early as 2015 to meet the forthcoming changes in nuclear security practices due to the rise of advanced nuclear technologies. The US Nuclear Energy Institute, a Washington, DC based policy organization of the nuclear technologies industry, published two white papers in November 2015 and December 2016, respectively, proposing new physical security requirements for advanced reactor concepts and urged the NRC to use the paper as a basis for rulemaking. NRC continues to collaborate with US nuclear industry officials as NRC works to undertake the rule-making cited previously.

Bilateral government-to-government cooperation in this area is another vehicle for ensuring operating States have the tools they need. The USA, for its part, provides a broad array of bilateral and multilateral nuclear security-related assistance. For decades, the US Department of Energy and NRC technical experts have engaged with foreign partners to help ensure the security of partners’ nuclear facilities and plans to continue this type of cooperation going forward as new reactor designs emerge. The USA engages bilaterally with nuclear cooperation partners as they consider the potential of advanced reactor technologies. In April 2021, the White House announced the USA’s most recent initiative in this regard at the Leaders’ Climate Summit: the Foundational Infrastructure for Responsible Use of Small Modular Reactor Technology (FIRST) programme. The FIRST programme provides capacity building support consistent with the IAEA Milestones Approach to enable partner countries to benefit from advanced nuclear technologies and meet their clean energy goals under the highest standards of nuclear security, safety and non-proliferation.

8.3.2 *Role of the IAEA*

In addition to the bilateral government-to-government and public–private sector partnerships described earlier, the IAEA will also need to play an integral role in assisting States, at their request, to meet their physical security obligations at advanced reactor facilities.

The IAEA should be prepared to provide advisory services through its International Physical Protection Advisory Service (IPPAS) and International Nuclear Security Advisory Service (INSServ) missions. It should also offer training to interested Member States on any identified specific challenges associated with advanced

²⁷United States Nuclear Regulatory Commission 2019.

reactor designs. Finally, the IAEA should also work to ensure that as users of these new technologies gain more experience globally, it will serve not only as the repository of that collective wisdom but also as an active disseminator of guidance and good practices to all users through various outreach activities. IAEA Member States must ensure that the IAEA has sufficient resources to develop needed guidance and provide appropriate training and advisory services to assist Member States who choose to access these technologies.

8.4 Conclusion

The forthcoming arrival of small modular reactors and other advanced nuclear reactor technologies can be an immensely beneficial development in the world's collective pursuit of energy security and meeting climate change objectives. For these technologies to successfully contribute to these goals, all stakeholders in the global civil nuclear cooperation community must be actively involved in this process. Fortunately, our existing global nuclear security-related legal regime is already properly designed to facilitate these benefits. In order to ensure that States can access these benefits, they must work collaboratively with supplier States, suppliers and the IAEA. It is only through the concerted and thoughtful efforts of everyone involved that we will ensure that as these new reactors come to market, the States operating them have the tools to ensure adequate physical security at their facilities.

References

- Bunn M, Holgate L, Kovchegin D, Tobey W (2020) IAEA Nuclear Security Recommendations (INFCIRC/225): The Next Generation. <https://www.stimson.org/2020/iaea-nuclear-security-recommendations-infcirc-225-the-next-generation>. Accessed 11 October 2021
- International Atomic Energy Agency (IAEA) (1975) The Physical Protection of Nuclear Material, INFCIRC/225. IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2009) Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10-G (Rev. 1). IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2011) Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA, Vienna
- International Atomic Energy Agency (IAEA) (2020), Preventive and Protective Measures Against Inside Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1). IAEA, Vienna
- United States Nuclear Regulatory Commission (2019) Physical Security for Advanced Reactors—Regulatory Basis for Public Comment.

The opinions expressed in this publication are those of the authors/editors and do not necessarily reflect the views of the IAEA: International Atomic Energy Agency, its Board of Directors, or the countries they represent.

Open Access This book is licensed under the terms of the Creative Commons Attribution 3.0 IGO license (<http://creativecommons.org/licenses/by/3.0/igo/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the IAEA: International Atomic Energy Agency, provide a link to the Creative Commons license and indicate if changes were made.

Any dispute related to the use of the works of the IAEA: International Atomic Energy Agency that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IAEA: International Atomic Energy Agency's name for any purpose other than for attribution, and the use of the IAEA: International Atomic Energy Agency's logo, shall be subject to a separate written license agreement between the IAEA: International Atomic Energy Agency and the user and is not authorized as part of this CC-IGO license. Note that the link provided above includes additional terms and conditions of the license.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.