# *Developing Regulatory Frameworks for A/SMRS: Security by Design (SEBD) and Other Regulatory Considerations*

**P. EFTEKHARI  
Primary Author   
Pacific Northwest National Laboratory (PNNL)**

**Washington, D.C., United States**

**Email: Pegah.eftekhari@pnnl.gov**

M. Man  
Contributor

Pacific Northwest National Laboratory (PNNL)   
Seattle, Washington

**Abstract**

The diversity of advanced and small modular reactor (A/SMR) designs, combined with various modes of deployment and specific circumstances with respect to a country’s threat assessment and design basis threat (DBT) or representative threat statement (RTS), raise new regulatory challenges and the need to adapt existing legislative and regulatory frameworks for nuclear security to account for the particularities of future A/SMR deployments. Establishing robust Security by Design (SeBD) regulatory requirements is essential for regulators and future operators to effectively address some of the potential security challenges posed by the future deployment and operation of A/SMRs. This paper discusses some of the regulatory challenges pertaining to the security of A/SMRs and embarks on a legal analysis of laws and regulations that illustrate how some of these challenges may be addressed. Based on open-source information, this paper analyzes legislative and regulatory provisions that could be leveraged to support SeBD and other security considerations for A/SMRs and identifies related references in International Atomic Energy Agency (IAEA) Nuclear Security Series publications. Based on the results of this analysis, the paper discusses several regulatory provisions that embarking and expanding countries may consider adding or enhancing in their frameworks as they further develop or adapt existing regulatory documents to the secure deployment of future A/SMRs. Among other topics, the analysis will focus on SeBD requirements and their consideration in the licensing process. (Released under **PNNL-SA-195386).**

1. ***Regulatory Challenges to Deployment of A/SMRs and Concept of Security by Design (SeBD)***

Advanced and Small Modular reactors (A/SMRs) incorporate[[1]](#endnote-1) specific attributes such as modularity and simplified design features that allow for higher reliability and passive and inherent safety features, capable of producing power output of 300 MW(e) or less[[2]](#endnote-2). According to the International Atomic Energy Agency (IAEA), there are currently more than 70 commercial SMR designs under development in 18 countries[[3]](#endnote-3). The concept of Security by Design (SeBD) particularly as it applies to A/SMRs has been an ongoing conversation among international organizations, government agencies, national regulators, and the commercial nuclear industry.

The IAEA Nuclear Security Series (NSS) No. 27-G or the Implementing Guide to INFCIRC/225/Rev. 5 defines SeBD as integrating physical protection principles as early as possible in a facility’s lifetime with the intent that the design provides the required level of security in a cost-effective way that is compatible with operations, safety, and nuclear material accounting and control. NSS No. 27-G further provides that SeBD is best implemented through a “structured approach in which a State’s nuclear security objectives are considered and fully taken into account in design decisions for the entire lifetime of the facility, starting with the planning of the facility and continuing through the design, construction, operational and decommissioning phases”[[4]](#endnote-4). On the other hand, the diversity of technology utilized in A/SMRs, their modularity and transportability to remote and off-grid locations with limited infrastructure, their usage of novel fuel types and autonomous control rooms, pose novel security challenges that the existing legislative and regulatory framework of many countries may not have contemplated or addressed yet. In addition, the synergies and relationship between designers, vendors, operators, and State’s relevant stakeholders will depend on the ownership and operational models of A/SMRs including Build-Own-Operate (BOO), Build-Own-Operate-Transfer (BOOT), or other leasing models. The A/SMRs deployment and organizational models may influence which States’ threat assessment, Design Basis Threat (DBT) or Representative Threat Statement (RTS) is utilized in designing the security features of the A/SMR and the security system of the new or expanding facility; in determining what security features should be included in the design of the A/SMRs, the host States’ confidentiality laws and regulations and their ability to share their DBT/RTS with foreign national vendors/designers and operators will also be implicated. The ownership and deployment model of A/SMRs will also affect which States’ regulatory licensing requirements and conditions would apply, particularly at the early stages of a facility’s lifecycle, *i.e., planning, siting, design, and construction.* Furthermore, open-source research reveals that many countries’ legislative and regulatory frameworks do not specifically contain provisions that require consideration of security in the early stages of a nuclear facility’s lifecycle including during planning, siting, design, and construction. Concurrently, and as elaborated below, the IAEA guidance publications such as NSS No. 27-G mainly address security considerations during the operation stage of a nuclear facility and other fundamental and recommendation level guidance including NSS No. 20 and 13 do not specially provide guidance on integrating SeBD principles, particularly as it applies to A/SMRs. To the extent that NSS No. 35-G offers action items during all stages of a facility’s lifecycle, this publication still does not provide detailed guidance regarding SeBD considerations for A/SMRs.

This paper seeks to first provide an overview of IAEA publications including NSS Nos. 20, 13, 27-G, 35-G, and the IAEA Nuclear Law Handbook; more specifically this analysis focuses on these publications’ guidance regarding safety-security interface, SeBD and other provisions that address the roles and responsibilities of nuclear security stakeholders such as States, competent authorities and operators to integrate security measures as early as possible in the lifetime of a nuclear facility. Based on these analyses, the paper then provides a series of recommendations to incorporate SeBD principles into regulatory licensing requirements governing new and expanding nuclear facilities, especially if deploying A/SMRs; these recommendations could be utilized and tailored by States’ competent authorities for inclusion into their licensing requirements as well as by the international community to modify and supplement existing international guidance, particularly as applicable to A/SMRs.

1. ***Overview of IAEA Nuclear Security Series and SeBD-Related Provisions***
2. **Objective and Essential Elements of a State’s Nuclear Security Regime, NSS No. 20**

NSS No. 20 provides States with a set of twelve essential elements for an effective and appropriate nuclear security regime, recognizing that the responsibility for implementing, maintaining, and sustaining a nuclear security regime rest entirely with the State. Under Essential Element 7, identification, and assessment of nuclear security threats, NSS No. 20, recommends that the State’s nuclear security regime is based on updated threat assessments and that internal and external nuclear security threats are identified and assessed, even if the target of an internal threat is extraterritorial[[5]](#endnote-5). The State’s threat assessment is in turn integral to the State’s identification and assessment of targets and potential consequences should they be compromised.[[6]](#endnote-6) NSS No. 20 requires the State to employ risk informed approaches in allocating its resources for nuclear security systems and measures as well as in conducting nuclear security activities, based on the concepts of graded approach and defense in depth[[7]](#endnote-7). All these concepts are integral to the States’ legislative and regulatory framework for nuclear security.

**SeBD and Safety-Security Interface**

Although NSS No. 20 does not specifically reference the concept of SeBD, in the introduction it emphasizes and highlights the importance of the safety-security interface to protection of persons, property, society, and the environment. It also states that security and safety measures “have to be designed and implemented in an integrated manner to develop synergy between these two areas” in a manner to ensure they do not compromise each other[[8]](#endnote-8). Thus, based on this guidance, States should consider incorporating SeBD principles by way of integrating the concept as part of their safety-security interface regulatory requirements and develop additional guidance for operators to address the novel threats associated with A/SMRs’ technologies.

1. **Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), NSS No. 13**

The INFCIRC/225/Revision 5 also known as the IAEA Nuclear Security Series No. 13, sets forth the IAEA’s recommendations on the physical protection of nuclear material and nuclear facilities. NSS No. 13 provides guidance to States in implementing a comprehensive physical protection regime for their nuclear material and nuclear facilities in keeping with their international obligations under the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment. NSS No. 13 describes the elements of a State’s physical protection regime, including its legislative and regulatory framework. Under Fundamental Principle A, NSS No. 13 provides that the responsibility for establishing, implementing and maintaining a physical protection regime “rests entirely with that State,” and it extends the State’s responsibility to ensure adequate protection for nuclear material to “international transport until that responsibility is properly transferred to another State[.][[9]](#endnote-9)” The State’s responsibility to establish a legislative and regulatory framework, governing the physical protection regime, includes defining requirements based on the threat assessment or DBT, as well as licensing requirements applicable to all nuclear material and nuclear facilities “regardless of whether [they are] under State or private ownership.[[10]](#endnote-10)” Fundamental Principle G on Threat, recommends the State develop threat assessments and DBTs relying on credible information sources, and to require operators, shippers and carriers to use threat assessments and DBTs as the basis for the design and implementation of the physical protection system. Finally, NSS No. 13, recommends that States establish confidentiality requirements for any information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities, specifically any information “addressing possible vulnerability in physical protection systems[.][[11]](#endnote-11)” However, NSS No. 13 does not provide the States with guidance on how to develop legislative and regulatory requirements that integrate security principles at the inception of A/SMRs’ design based on the States’ current threat assessment and DBT. States would also benefit from additional international guidance on developing memorandum of understandings or other similar agreements that could govern the mechanism(s) and extent to which they could share their threat assessment and DBTs with foreign national designers, operators, shippers, and carriers of A/SMRs, without violating their confidentiality requirements.

**SeBD and Safety-Security Interface**

Although NSS No. 13 does not explicitly label the concept as SeBD, under Fundamental Principle E on responsibilities of the operators, it recommends that physical protection is taken into account for “site selection and design” of “new nuclear facilities[,]” “as early as possible” and that “ the interface between physical protection, safety and nuclear material accountancy and control” is addressed to avoid any conflicts and to ensure that all elements support each other[[12]](#endnote-12). In addition, under recommendations for physical protection against unauthorized removal of nuclear material in use and storage and sabotage, NSS No. 13 recommends the operator “assess and manage the physical protection interface with safety and nuclear material accountancy and control activities” to ensure that they do not adversely affect each other and that they are mutually supportive to the extent possible[[13]](#endnote-13). NSS No. 13 also advises that the State put in place contingency plans to address the safety and security interface, specifically as they relate to locating and recovering missing or stolen nuclear material[[14]](#endnote-14). The guidance to address the interface of safety and security as part of contingency planning extends to transport security and responsibilities of carriers and other entities charged with locating and recovering missing or stolen nuclear material during transport[[15]](#endnote-15).

Finally, and with respect to response and measures to minimize and mitigate radiological consequences of sabotage, NSS No. 13 recommends the State assess and validate, through joint exercises, “the adequacy of the interfaces” and the coordination between emergency and security organizations to respond to threat scenarios and their ability to incorporate lessons learned to improve their management systems[[16]](#endnote-16). The same guidance extends to testing of emergency and contingency plans addressing transport security to ensure that it adequately address the safety and security interface[[17]](#endnote-17). Thus, by recommending operators address physical protection (*i.e.,* security) at the time of site selection and design for new nuclear facilities and urging them to avoid conflicts between safety, security, and safeguards (3S), NSS No. 13 arguably recommends that States incorporate SeBD principles into their licensing and regulatory requirements during the operation stage[[18]](#endnote-18). However, additional guidance may be required to address integration of SeBD principles and the security elements, equipment and systems that fall within the safety-security interface during the planning, siting, design, and construction stages of a nuclear facility that may also incorporate A/SMRs. Moreover, to the extent that A/SMRs’ features such as autonomous control room, modularity, and deployment to remote and off-grid locations with inadequate emergency and response infrastructure may require additional security measures, NSS No. 13 does not offer guidance to operators.

1. **Implementing Guide on Physical Protection of Nuclear Material and Nuclear Facilities, NSS No. 27-G**

The IAEA NSS No. 27-G or the Implementing Guide to INFCIRC/225/Rev. 5 provides guidance to States on establishing, implementing, and sustaining a physical protection regime for nuclear material and nuclear facilities. NSS 27-G states, in pertinent part, that if a State “accepts nuclear material and nuclear facilities within its borders, that State has also accepted *responsibility* for the protection of those material from unauthorized removal and … from sabotage[.]”[[19]](#endnote-19) To satisfy this responsibility, the State’s risk management approach should address its assessment of threats and DBT, as well as the potential consequences of sabotage and unauthorized removal and target vulnerabilities. The State’s responsibility for establishing a legislative and regulatory framework governing its physical protection regime extends to the “introduction of new types of nuclear material and nuclear facilities.[[20]](#endnote-20)” States could employ three distinct regulatory approaches, including the prescriptive approach, performance-based approach, and the combined approach[[21]](#endnote-21) to specify the regulatory requirements addressing the State’s threat assessment and DBT. Under the performance-based approach, the operator utilizes the DBT to design the physical protection system, and the competent authority evaluates the same based on the DBT. Under the prescriptive approach, a threat assessment may be sufficient for the competent authority to define the physical protection measures that the operator will be required to implement exactly[[22]](#endnote-22). In the combined approach, a combination of these approaches is utilized. The State is also responsible for setting licensing requirements in relation to physical protection systems, as well as for issuance, renewals, and amendment of existing licenses throughout the lifecycle of a nuclear facility. Finally, the State is responsible for defining regulatory enforcement measures as part of its physical protection regime and to enforce compliance with its regulatory requirements. Therefore, additional international guidance is needed to address how the ownership and operational models of A/SMRs impact which State’s regulatory licensing and enforcement requirements would apply to licensing of A/SMRs at the planning, siting, design, and construction stages. In addition, for States that utilize a performance-based approach, additional international guidance regarding the mechanism and extent to which threat assessment and DBT must be shared with designers to integrate security principles into the design of the A/SMRs would be valuable.

**SeBD and Safety-Security Interface**

NSS No. 27-G introduces the concept of SeBD and recommends the operators take nuclear security into consideration at the time of the “design of new nuclear facilities”[[23]](#endnote-23). The intent for the concept of SeBD is to design a new nuclear facility by providing the required level of security in a cost-effective way, compatible with operations, safety and NMAC[[24]](#endnote-24), while simplifying the task of maintaining an effective physical protection system over the lifetime of the facility[[25]](#endnote-25). SeBD is best implemented through a structured approach in which “a State’s nuclear security objectives are considered and fully taken into account in design decisions for the entire lifetime of the facility, starting with the planning of the facility and continuing through the design, construction, operational and decommissioning phases[[26]](#endnote-26).” NSS No. 27-G identifies a good practice to incorporate SeBD principles as “integrat[ing] the design of the physical protection system into the overall design of the nuclear facility as early as possible in the process.” These early considerations should include decisions regarding facility siting and layout, how they may impact the design and effectiveness of physical protection systems, and to minimize conflicts with other design requirements while taking advantage of engineering solutions to make the design more complementary and synergetic[[27]](#endnote-27).

With respect to the safety-security interface, NSS No. 27-G requires the State’s nuclear security regime to provide for “appropriate management of the interfaces between physical protection and nuclear material accounting and control and between physical protection and safety[,]” in a manner to avoid conflict between safety and security and to ensure the two complement each other[[28]](#endnote-28). More specifically, under assignment of physical protection responsibilities, NSS No. 27-G, places the onus on the State to assign responsibilities to relevant competent authorities and governmental entities to manage the interfaces of safety-security and NMAC[[29]](#endnote-29). With respect to the operator’s responsibilities, NSS No. 27-G highlights the importance of taking security into consideration at the site selection and design stages of a new nuclear facility and addressing the safety and security interface[[30]](#endnote-30), and elaborates that “[l]ocal infrastructure, site layout and other local conditions might all influence nuclear security. Site layout, particularly for nuclear facilities with multiple nuclear installations, may need to account for the space requirements of the physical protection measures to provide adequate defense in depth.[[31]](#endnote-31)” Furthermore, NSS No. 27-G recommends the organization’s integrated security management system clarify responsibilities regarding the safety-security interface[[32]](#endnote-32). More specifically, NSS No. 27-G provides additional guidance on operator’s responsibilities to assess and manage the interface between physical protection, safety and NMAC activities, to avoid conflicts, and ensure compatibility to the extent possible, by recommending operators to:

* Establish and maintain effective management of the interface[[33]](#endnote-33).
* Adopt, through the integrated management system, an integrated and coordinated approach to review any proposed safety or security changes prior to implementation to ensure that they do not result in unintended degradation of arrangements in the other area and to communicate any possible adverse interactions to the appropriate personnel to initiate compensatory/mitigating actions[[34]](#endnote-34).
* Utilize safety-security review boards, work planning and controls, and configuration management to identify safety-security interface issues and appropriately manage them during design, construction, operation, nuclear security events and emergencies[[35]](#endnote-35), and decommissioning[[36]](#endnote-36).
* Ensure that physical protection personnel are notified of changes to:

a) the nuclear facility’s physical layout;

b) configuration of facilities, structures, systems, and components; and

c) facility’s operation or emergency planning. Any such changes should be reviewed prior to implementation[[37]](#endnote-37).

* Ensure that safety personnel are notified and to conduct a review of any changes to the physical protection measures[[38]](#endnote-38).
* Effectively manage the safety-security interface, ensuring that they are mutually supportive (*e.g*., through reductions in inventories of nuclear material and other hazard reduction measures, adequate physical separation of safety equipment to provide redundancies)[[39]](#endnote-39).

Although NSS No. 27-G provides some guidance regarding the safety-security interface and the importance of incorporating SeBD principles by taking facility siting, layout and its impact on the design and effectiveness of physical protection systems into consideration as early as possible, it does not offer specific guidance on how A/SMRs’ modularity and need for more frequent refueling cycles for example, may influence the design of physical protection systems at the planning, siting, design and construction stages of a facility. In addition, NSS No. 27-G provides guidance to operators regarding integrated security management approaches, which rely on knowledgeable safety and security personnel and collaborative and coordinated review and notification processes to ensure that any changes to the nuclear facility’s physical layout, configuration of facilities, structures, systems and components, and facility’s operation or emergency planning is timely communicated to other relevant personnel; this guidance however should be supplemented to account for particularities of A/SMRs’ technologies and to provide additional guidance on integrated security management approaches to communicate any such changes during the planning, siting, design and construction stages of the facility’s lifecycle.

1. **Implementing Guide on Security During the Lifetime of a Nuclear facility, NSS No. 35-G**

NSS No. 35-G provides guidance (including action items) on security measures to States, competent authorities and operators, during, and while in transition between, the 8 stages in the lifetime of a nuclear facility encompassing the planning, siting, design, construction, commissioning, operation, cessation of operation and the decommissioning stages[[40]](#endnote-40). NSS No. 35-G draws attention to the importance of addressing nuclear security early in the design of a new facility and during partial redesigns and modification to capture efficiencies and effectively address the interface of safety, safeguards, and operations; similarly important is to address nuclear security consideration during commissioning and operation and the decommissioning stages[[41]](#endnote-41). Significantly, NSS No. 35-G highlights that although NSS Nos. 20, 13, and 27-G provide guidance on integrating security measures as early as possible in the lifetime of a facility, “they focus primarily on security during the operation of a facility, and not on nuclear security measures during all stages in the lifetime of a nuclear facility.[[42]](#endnote-42)” In light of this gap, what follows is a summary of goals and certain action items for operators, State and competent authorities from the guidance provided in NSS No. 35-G that could be utilized to incorporate SeBD principles during the first four stages of planning, siting, design and construction[[43]](#endnote-43) of a nuclear facility’s lifecycle.

**Planning Stage**: At the planning stage the relevant stakeholders should ensure that: a) the State’s nuclear security regulatory requirements are met; b) security measures are integrated with operational and safety requirements (*i.e.,* safety-security interface); and c) communication frameworks among relevant safety, security, safeguards, and facility operations stakeholders are established. Some relevant action items during this stage include:

* The operator should develop a nuclear security strategy that meets State requirements[[44]](#endnote-44).
* The operator should promote awareness of nuclear security and conduct nuclear security training for all organizations and individuals involved in facility planning, *i.e., safety, operational, safeguards personnel[[45]](#endnote-45).*
* The operator should coordinate its nuclear security planning activities with the planning activities associated with nuclear safety, safeguards, and facility operations to avoid or resolve conflicts and to find synergies[[46]](#endnote-46).
* The operator should plan for measures to protect sensitive information consistent with State and competent authority requirements, including confidentiality measures and procedures to limit access to sensitive information to those who have a need to know to perform their duties[[47]](#endnote-47).

**Siting Stage**: Because the location of the facility could potentially elevate or decrease vulnerabilities to external security threats and the associated consequences with malicious activity, stakeholders should take nuclear security and safety considerations into account concurrently with seismic activity, geology, meteorology and hydrology and neighboring States’ concerns[[48]](#endnote-48). Thus, relevant stakeholders would need to evaluate local and regional threats, security interfaces and interdependencies with existing nuclear facilities, impact on nearby populated areas and infrastructure, availability of response force and space for site reconfiguration based on security needs[[49]](#endnote-49). Some relevant action items during this stage include:

* The State should examine treaties, agreements, security conditions and relationships with neighboring States to determine their potential impact on site selection[[50]](#endnote-50).
* The competent authority should require that nuclear security considerations, including information on national and local threats, be considered during site selection[[51]](#endnote-51).
* The operator should take into account nuclear security considerations, such as information on national and local threats, in the site selection process[[52]](#endnote-52).
* The operator should evaluate the availability of infrastructure for effective nuclear security, including the availability of response forces for a nuclear security event[[53]](#endnote-53).

**Design Stage:** Relevant stakeholders should implement measures that“strengthen synergy between [safety and security] areas” taking advantage of synergistic design and collaborative design teams comprised of safety and security personnel, as well as minimizing potential conflict with safety, safeguards, and facility operations by identifying and resolving regulatory requirements’ conflicts during the design stage[[54]](#endnote-54). Some relevant action items during this stage include:

* The competent authority should ensure that any design modifications remain in compliance with applicable regulatory requirements for nuclear security and safety[[55]](#endnote-55).
* The competent authority should conduct a technical assessment of the final design of a facility to ensure that it meets applicable requirements for nuclear security and safety before licensing activities or granting authorization[[56]](#endnote-56).
* The operator should coordinate nuclear security measures to be incorporated in the design with measures to be incorporated for other disciplines (*e.g.,* safety, safeguards, and operations) to compare relevant regulatory requirements, identify synergies and resolve potential conflicts[[57]](#endnote-57).
* The operator should review all aspects of the design to ensure the appropriate inclusion of nuclear security measures[[58]](#endnote-58).

**Construction Stage**: the stakeholders should ensure that: a) the nuclear security measures’ construction and installation satisfy regulatory requirements and meet DBT/RTS; b) interim security vulnerabilities that may be present during the construction stage are addressed; c) organization(s) is established to conduct nuclear security responsibilities during and after construction; and d) functional, operational and performance testing of equipment and systems/components are performed. Some relevant action items during this stage include:

* The State should develop a comprehensive national response plan for nuclear security events if this plan does not already exist[[59]](#endnote-59).
* The competent authority should review and approve the operator’s security measures and plans, if required, prior to the start of construction[[60]](#endnote-60).
* The operator should implement a management system that integrates nuclear security into the overall management system of the facility[[61]](#endnote-61).
* The operator should implement a configuration management program to ensure that any design changes undertaken during construction do not affect the facility’s ability to meet regulatory requirements for nuclear security[[62]](#endnote-62).
* The operator should implement and conduct nuclear security training activities for all personnel with security responsibilities. All facility personnel should receive basic security awareness training[[63]](#endnote-63).

Thus, although NSS No. 35-G offers valuable guidance in terms of action items and goals to States, competent authorities and operators that integrate security principles for each stage of a nuclear facility’s lifecycle, additional detailed guidance is desirable for the relevant stakeholders before they can modify and tailor these action items into licensing and other regulatory requirements, particularly as it relates to A/SMRs. In other words, for States contemplating deployment of A/SMRs, NSS No. 35-G does not offer guidance with respect to specific challenges imposed by A/SMRs’ technologies, use of novel fuel types, transportability to remote and off-grid locations, and limitations that States face in sharing their threat assessment and DBT with other States or foreign national vendors and designers.

1. **Handbook on Nuclear Law, Implementing Legislation, Volume II**

Chapter 14 of theHandbook on Nuclear Law, Vol. II (*hereinafter* “the Handbook”), last updated in 2003, provides model provisions for nuclear security. Although the Handbook does not specifically reference SeBD or safety-security interface, it does recognize the importance of the concept of 3S (safety, security, and safeguards) at the outset and encourages legislatures to avoid gaps, overlaps and inconsistencies in drafting laws. Although Chapter 6 of the Handbook provides model provisions focused on the safety of nuclear facilities and decommissioning, some of these provisions related to the licensing of a new facility have relevance to security. In particular, the Handbook recommends that primary responsibility for safety and security of the facility is placed on the licensee and that the approval of a site should be based upon requirements of the law and any applicable regulations. Chapter 6 also recommends that the regulatory body shall review and assess the basic design of the proposed facility, to confirm that it can meet relevant safety, security, and physical protection requirement. Chapter 14 provides model provisions on regulating physical protection, responsibilities of the licensee, international cooperation and assistance, protection of confidential information and communications that prejudice security, nuclear security, and nuclear facility related offenses, and establishing jurisdiction. However, the Handbook’s model provisions in Chapter 14 do not provide guidance to States on addressing safety-security interface and on integration of SeBD principles. Nor does the Handbook offer guidance to States on modifying their regulatory licensing requirements to address security for A/SMRs. Thus, a revised version of the Handbook containing model SeBD provisions for States’ legislatures and regulatory authorities, as well as additional guidance to operators regarding integration of security principles into the physical protection systems during early stages of a nuclear facility’s lifecycle, particularly as applicable to A/SMRs could be very beneficial.

1. ***Recommendations and Next Steps***

Based on the analyses above, the author provides a series of recommendations that if incorporated into licensing and other regulatory requirements or regulatory guidance applicable during the planning, siting, design, or construction stages of a nuclear facility’s lifecycle, will promote integration of SeBD principles as early as possible, particularly as applied to A/SMRs. It is worth noting that some States require a distinct license for each stage of a nuclear facility’s lifecycle while others may extend the same license for the entire lifecycle of a facility, with some additional conditions. The diversity of States’ regulatory licensing frameworks and approaches, insufficient clarity on the safety-security interface and the relevant security considerations, the novel challenges imposed by A/SMRs’ technologies, and the limitations that States face in sharing their threat assessment and DBTs with foreign national designers of A/SMRs (as discussed *supra*), make it more pressing for the States and the international community to develop further guidance on regulatory model provisions that incorporate SeBD principles for each stage of a nuclear facility’s lifecycle. Furthermore, if SeBD principles are integrated into licensing and other regulatory requirements during early stages of a nuclear facility’s lifecycle, operators and ultimately regulators can expect significant cost savings and efficiencies. Early consideration of security measures will also enable the operators to create synergies between security, safety, safeguards, and operational management at the facility, avoiding significant costs associated with retrofitting during the operational stage. Below are some recommendations that may be utilized and tailored by States into regulatory licensing requirements particularly for the planning, siting, design, and construction stages of a nuclear facility’s life cycle. These recommendations can equally be taken into consideration by the international community and the IAEA for modification and incorporation into the nuclear security series guidance and/or additions to model provisions contained in the Handbook on Nuclear Law. The recommendations below are for consideration by the State, the regulatory body, and the operators:

* Providing guidance in terms of agreement, mechanisms, and extent to which threat assessment and DBTs may be shared through Memorandum of Understandings (MOUs) and confidentiality agreements between States, designers, and vendors without violating the States’ confidentiality laws and regulations during the planning, siting, design, and construction stages of a nuclear facility for deployment of A/SMRs.
* Providing guidance on how the ownership and operational models of A/SMRs impacts applicability of the State’s regulatory, licensing and enforcement requirements for purposes of licensing A/SMRs at the planning, siting, design, and construction stages.
* Providing a definition for safety-security interface and requiring nuclear facilities (new or expanding) to define the systems, components, and equipment and physical protection features, including that of A/SMRs, that fall within the safety-security interface as early as during the planning stage and continuing through siting, design, and construction, as well as during the commissioning, operation, and decommissioning stages.
* Providing for formal and informal opportunities where applicants for a license (preferably as early as during the planning and siting stages of a facility’s lifecycle) can engage in discussions with the regulatory authority regarding regulatory expectations on integrating SeBD into the design of the physical protection systems and its components, *i.e.,* pre-licensing assessments of safety-security interface.
* Developing guidance for applicants for a license (preferably as early as during the planning and siting stages of a facility’s lifecycle) on the process, notice requirements, required information and technical documentation applicable to the pre-licensing assessments of safety-security interface.
* Requiring establishment of safety-security interface committee(s) comprising of personnel with competencies in safety, security, safeguards, NMAC and operations, and knowledgeable on A/SMR technologies and safety-security features; this committee should be formed as early as possible, preferably during the planning stage and may continue its operation through the lifecycle or for specific stages including planning, siting, design, and construction.

* Defining a process for review and assessment of any proposed changes to safety and security systems/components/equipment as well as physical protection design, timelines for any such review and assessment and processes to follow before any such changes are implemented, including changes caused by A/SMRs technologies and designs.
* Defining a process for communication of potential changes to safety-security systems, components, and equipment including what, when and the range of stakeholders to whom any such information should be communicated to; this process should be utilized to ensure that any changes to the nuclear facility’s physical layout, configuration of facilities, structures, systems and components, and facility’s operation or emergency planning is timely communicated to all relevant external and internal stakeholders including safety and security personnel. This process is also particularly important to ensure that in the event of changes to security features, safety experts review any new definitions for the threshold for unacceptable radiological consequences or changes in operations or threats, applicable to sabotage targets.
* Defining and requiring that safety-security review boards, work planning and controls, and configuration managements be utilized to identify safety-security interface issues and to appropriately manage them during design, construction, operation, nuclear security events and emergencies, and decommissioning. Additional guidance is required to address how A/SMRs technologies and their use of novel fuel types, more frequent refueling cycles, modularity, deployment to remote and off-grid locations with limited emergency and response infrastructure, among others, may create additional safety-security interface issues.
* Requiring the operators to develop a nuclear security strategy at the planning stage, which includes their processes and approaches to raising awareness about safety-security interface, SeBD, and A/SMRs’ specific safety-security features through training for all organizations and individuals involved in facility planning, *i.e., safety, operational, safeguards and security personnel.*
* Requiring nuclear facilities (new or expanding) to establish and adopt an integrated management system, particularly during siting and design stages, that employs an integrated and coordinated approach to review any proposed safety or security changes prior to implementation to ensure that they do not result in unintended degradation of arrangements in the safety and security areas, including for A/SMRs, and to communicate any possible adverse interactions to the appropriate personnel to initiate compensatory/mitigating actions.
* Requiring nuclear facilities (new or expanding) to establish clear guidelines for training and continuity of knowledge for the safety-security committee experts during each stage of a nuclear facility’s lifecycle, particularly beginning at the siting and design stages and onward through the facility’s lifecycle.
* Requiring nuclear facilities (new or expanding) to integrate analysis and assessment of safety-security interface with seismic activity, geology, meteorology and hydrology and neighboring States’ threat concerns and submit their analysis for evaluation to the relevant stakeholders/competent authorities, particularly at the planning and siting stages. This analysis and assessment should include local and regional threats, security interfaces and interdependencies with existing nuclear facilities, impact on nearby populated areas and infrastructure, availability of response force and space for site reconfiguration based on security needs, among other consideration as specified by the State and competent authorities and as dictated by A/SMRs’ technologies.
* Requiring nuclear facilities to establish through processes, procedures and protocols approaches for effective management of the safety-security interface to ensure mutually supportive measures are undertaken and that conflicts are minimized and avoided, particularly during the siting and design stages and indicate how any such management approaches are different for A/SMRs; effective management approaches should include facility’s policy and procedure on forming its safety-security committee, establishment of lines of responsibilities for the committee experts, and interactions with other personnel at the facility.
* Requiring nuclear facilities (new and expanding) to provide as part of their basic generic decision or final design of the facility, particularly at the planning, siting, and design stages, the engineering solutions that were utilized to make the design more complementary and synergetic with respect to the safety-security interface.
* Requiring nuclear facilities (new and expanding) to establish and maintain synergistic design and collaborative design teams comprised of safety and security personnel, to minimize potential conflicts with safety, safeguards, and facility operations by identifying and resolving regulatory requirements’ conflicts during the design stage. The analyses and modifications to design as well as the final design of the facility should be submitted to the relevant competent authority for technical assessment to ensure that it meets applicable regulatory nuclear security and safety requirements before licensing.
* Requiring nuclear facilities (new and expanding) to establish that the safety-security interface components, systems, and equipment comply with regulatory and DBT/RTS requirements with respect to their construction and installation as well as showing that any interim security vulnerabilities, present during the construction stage are addressed.
* Requiring nuclear facilities (new and expanding) to establish and maintain integrated management organization(s) to conduct safety-security interface responsibilities during and after the construction stage.
* Requiring nuclear facilities (new and expanding) to conduct functional, operational and performance testing of safety-security interface equipment, systems, and components including for A/SMRs during the construction stage and through operations.

1. ***Conclusion***

Incorporation of the SeBD principles, either as standalone requirements or as part of the safety-security interface, will require additional guidance from the international community, the States, and the regulatory authorities, particularly for A/SMR technologies. The above-mentioned recommendations provide a path ahead for the stakeholders to consider creating guidance and applicable processes as early as possible in the nuclear facilities’ lifecycle beginning at the planning and siting, and continuing through design and construction stages that would incentivize the operators to integrate security into the physical protection systems’ design with safety and operational requirements.

1. ***Acknowledgment***

The author would like to thank the U.S. Department of Energy, National Nuclear Security Administration’s Office of International Nuclear Security for sponsoring this research.

1. Advanced Reactors are fission reactors with significant improvements compared to reactors operating on the date of enactment, or a reactor using nuclear fusion, *see* the US Energy Act of 2020. [↑](#endnote-ref-1)
2. Based on their core design current SMR technologies are: High Temperature Gas Cooled Reactors (HTR), fast Neutron Reactors (FNRs), light Water Reactors (LWRs), and Molten Salt Reactors (MSRs), see https://www.iaea.org/topics/small-modular-reactors; see also https://www.iaea.org/topics/small-modular-reactors#:~:text=These%20reactors%20have%20advanced%20engineered,SMR%20designs%20and%20concepts%20globally. [↑](#endnote-ref-2)
3. see Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactor Information System (ARIS), 2022, available at: https://aris.iaea.org/Publications/SMR\_booklet\_2022.pdf [↑](#endnote-ref-3)
4. NSS No. 27-G, 1.6, 4.8-4.9 [↑](#endnote-ref-4)
5. NSS No. 20, 3.7 [↑](#endnote-ref-5)
6. NSS No. 20, Essential Element 8 [↑](#endnote-ref-6)
7. NSS No. 20, Essential Element 9 [↑](#endnote-ref-7)
8. NSS No. 20, 1.2 [↑](#endnote-ref-8)
9. NSS No. 13, Fundamental Principle B states that the State’s responsibility should be determined “either by the borders of its sovereign territory or the flag of registration of the transport vessel or aircraft.” And that State’s physical protection regime should retain jurisdiction and continuous control over nuclear material in transport with clearly defined lines of responsibilities among the involved States. [↑](#endnote-ref-9)
10. NSS No. 13, 3.11 [↑](#endnote-ref-10)
11. NSS No. 13, 3.54 [↑](#endnote-ref-11)
12. NSS No. 13, 3.28 and 5.18 [↑](#endnote-ref-12)
13. NSS No. 13, 4.11 [↑](#endnote-ref-13)
14. NSS No. 13, 4.52 [↑](#endnote-ref-14)
15. NSS No. 13, 6.47 and 6. 63 [↑](#endnote-ref-15)
16. NSS No. 13, 5.52 [↑](#endnote-ref-16)
17. NSS No. 13, 6.68 [↑](#endnote-ref-17)
18. Although NSS No. 13 provides guidance that is generally applicable to the operation stage of a nuclear facility’s lifecycle, certain security measures, if modified and tailored, may be equally applicable during design and construction stages as well. [↑](#endnote-ref-18)
19. NSS No. 27-G, 2.2, italics added for emphasis. [↑](#endnote-ref-19)
20. NSS No. 27-G, 3.7 [↑](#endnote-ref-20)
21. NSS No. 27-G, 3.59 [↑](#endnote-ref-21)
22. See NSS No. 27-G, 3.59, except where Category I nuclear material is held and/or the sabotage of the nuclear facility could potentially lead to high radiological consequences. [↑](#endnote-ref-22)
23. NSS No. 27-G, 4.8 [↑](#endnote-ref-23)
24. NSS No. 27-G, 4.9 [↑](#endnote-ref-24)
25. NSS No. 27-G, 4.8 [↑](#endnote-ref-25)
26. NSS No. 27-G, 4.9 [↑](#endnote-ref-26)
27. NSS No. 27-G, 4.10 [↑](#endnote-ref-27)
28. NSS No. 27-G, 3.2 [↑](#endnote-ref-28)
29. NSS No. 27-G, 3.8 (e-f) [↑](#endnote-ref-29)
30. NSS No. 27-G, 4.7 [↑](#endnote-ref-30)
31. NSS No. 27-G, 4.7 [↑](#endnote-ref-31)
32. NSS No. 27-G, 4.14 [↑](#endnote-ref-32)
33. NSS No. 27-G, 4.147 [↑](#endnote-ref-33)
34. NSS No. 27-G, 4.148 [↑](#endnote-ref-34)
35. NSS No. 27-G, 4.150 addresses a range of safety-security interface issues that may arise during nuclear security events and emergencies including: a) coordination between the security and safety response in connection to a nuclear security event and any emergencies resulting from it; b) ensuring that security response forces are familiar with the facility and its layout, location of nuclear material and safety equipment/systems and are trained on radiation protection requirements; c) providing for radiation protection of response forces as they respond to a sabotage attack; d) providing for protection of safety responders and facility personnel should they be present in a contaminated area during security force’s response to a nuclear security event; e) utilizing special physical protection arrangements to ensure that physical protection barriers do not compromise personnel’s ability to evacuate areas in the event of fire, criticality or radiological release; f) adequately considering the need for off-site emergency responders and vehicles to quickly enter to provide medical and other urgent assistance when determining the level of necessary inspections and searches before gaining access to protected areas. [↑](#endnote-ref-35)
36. NSS No. 27-G, 4.149 [↑](#endnote-ref-36)
37. NSS No. 27-G, 4.152 [↑](#endnote-ref-37)
38. This is particularly important to ensure that safety experts review any new definitions for the threshold for unacceptable radiological consequences or changes in operations or threats, applicable to sabotage targets. NSS No. 27-G, 4.152 [↑](#endnote-ref-38)
39. NSS No. 27-G, 4.153 [↑](#endnote-ref-39)
40. NSS No. 35-G, 1.1-1.4 [↑](#endnote-ref-40)
41. NSS No. 35-G, 1.1 [↑](#endnote-ref-41)
42. NSS No. 35-G, 1.2-1.3 [↑](#endnote-ref-42)
43. The author selected these four stages because these are the earlier stages in a facility’s Lifecyle for which NSS No. 27-G does not offer guidance on and due to the space limitations of this paper. [↑](#endnote-ref-43)
44. NSS No. 35-G, Action 1-17 [↑](#endnote-ref-44)
45. NSS No. 35-G, Action 1-18 [↑](#endnote-ref-45)
46. NSS No. 35-G, Action 1-20 [↑](#endnote-ref-46)
47. NSS No. 35-G, Action 1-22 [↑](#endnote-ref-47)
48. NSS No. 35-G, 3.9 [↑](#endnote-ref-48)
49. NSS No. 35-G, 3.10 [↑](#endnote-ref-49)
50. NSS No. 35-G, Action 2-1 [↑](#endnote-ref-50)
51. NSS No. 35-G, Action 2-4 [↑](#endnote-ref-51)
52. NSS No. 35-G, Action 2-6 [↑](#endnote-ref-52)
53. NSS No. 35-G, Action 2-8 [↑](#endnote-ref-53)
54. NSS No. 35-G, 3.13-3.14 [↑](#endnote-ref-54)
55. NSS No. 35-G, Action 3-3 [↑](#endnote-ref-55)
56. NSS No. 35-G, Action 3-4 [↑](#endnote-ref-56)
57. NSS No. 35-G, Action 3-10 [↑](#endnote-ref-57)
58. NSS No. 35-G, Action 3-12 [↑](#endnote-ref-58)
59. NSS No. 35-G, Action 4-1 [↑](#endnote-ref-59)
60. NSS No. 35-G, Action 4-2 [↑](#endnote-ref-60)
61. NSS No. 35-G, Action 4-6 [↑](#endnote-ref-61)
62. NSS No. 35-G, Action 4-10 [↑](#endnote-ref-62)
63. NSS No. 35-G, Action 4-13 [↑](#endnote-ref-63)