NUCLEAR SECURITY SERIES No. 10-G (Rev. 1)

NST058 (Revision of NSS 10)

DRAFT: March 2 2018

Step 8: Soliciting comments by Member States

NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The objective of a State's nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event. [1].

1.2. The Nuclear Security Fundamentals set out the objective of a nuclear security regime and its essential elements [1]. The Nuclear Security Recommendations indicate what a nuclear security regime should address regarding:

(a) Physical Protection of Nuclear Material and Nuclear Facilities [2];

(b) Radioactive Material and Associated Facilities [3]; and

(c) Nuclear and Other Radioactive Material out of Regulatory Control [4].

1.3. The first version of this Implementing Guide was issued in 2009. The current revision updates this publication to take into account developments in the field as well as to ensure consistency in terminology with Refs. [1] – [4], which were published after 2009.

1.4. This publication has also been updated relative to the first edition to include physical and cyber threat considerations, to clarify the use of a threat assessment as an alternative approach to the design basis threat as recommended in Ref. [2], to sufficiently explain how to develop application specific design basis threats and to better address threats using or supported by cyber capabilities.

OBJECTIVE

1.5. The objective of this publication is to provide a detailed step by step methodology for performing a nuclear security threat assessment and for the development, use and maintenance of design basis threats and representative threat statements. This includes:

(a) Defining the roles and responsibilities of the State, competent authorities, including the regulatory body[1], and operators;

(b) Identifying and assessing threats related to nuclear security;

(c) Developing threat statements such as design basis threats and/or representative threat statements using the results of a nuclear security threat assessment;

(d) Using design basis threats and/or representative threat statements to develop nuclear security systems and measures, and nuclear security requirements;

(e) Maintaining the nuclear security threat assessment documentation; and

(f) Maintaining design basis threats and representative threat statements.

1.6. This publication is intended for use by States, competent authorities, including the regulatory body, and the operators of facilities and activities associated with nuclear and other radioactive material, including shippers and carriers.

SCOPE

1.7. The concept and methodology described in this publication applies to the performance of nuclear threat assessments and for development, use and maintenance of design basis threats and representative threat statements for protecting nuclear and other radioactive material as well as associated facilities and activities.

1.8. Guidance for developing a risk informed approach and conducting threat and risk assessments as the basis for the design and implementation of sustainable nuclear security systems and measures for the prevention of, detection of, and response to criminal or intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control is not provided in this publication. Guidance on this topic can be found in *Risk Informed*

[1] While some States may have multiple regulatory bodies responsible for nuclear and other radioactive material and associated facilities and activities, for simplicity, in this publication we refer to regulatory body in the singular.

Approach to Nuclear and Other Radioactive Material out of Regulatory Control (NSS No. 24-G) [5].

STRUCTURE

1.9. Following this introduction, Section 2 addresses nuclear security threat assessment in a risk informed approach. Section 3 provides an overview of the process of performance of nuclear security threat assessment, and the development, use and maintenance of nuclear security threat assessment documentation, design basis threats and representative threat statements. Section 4 outlines the roles and responsibilities of the organizations involved into the nuclear security threat assessment process, Section 5 provides guidance on how to perform a nuclear security threat assessment, Section 6 describes the development of threat statements, and Section 7 provides guidance on the use of threat statements. Finally, Section 8 provides guidance on the maintenance of the nuclear security threat assessment documentation and the threat statements. A model for a design basis threat is provided as an annex.

2. NUCLEAR SECURITY THREAT ASSESSMENT IN A RISK INFORMED APPROACH

2.1. Both international conventions and IAEA Nuclear Security Series guidance underscore the importance of threat assessment and the use of a risk-informed approach to nuclear security. Notably, according to Fundamental Principle G (Threat) of the Convention on the Physical Protection of Nuclear Material (CPPNM) [6, 7], as amended, "the State's physical protection should be based on the State's current evaluation of the threat."

2.2. Moreover, according to Essential Element 7 of Ref. [1],

"A nuclear security regime uses risk informed approaches, including in the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth, which take into account the following:

(a) The State's current assessment of the nuclear security threats, both internal and external;

(b) The relative attractiveness and vulnerability of identified targets to nuclear security threats;

(c) Characteristics of the nuclear material, other radioactive material, associated facilities and associated activities;

(d) Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, associated activities, sensitive information or sensitive information assets, and other acts determined by the State to have an adverse impact on nuclear security."

2.3. Furthermore, according to Ref. [2], "the State should define requirements - based on the threat assessment or design basis threat - for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal or sabotage," and according to Ref [3], "the State should assess its national threat to radioactive material, associated facilities and associated activities, and should periodically review its national threat, and evaluate the implications of any changes in the threat for the design or update of its nuclear security regime." Ref [3] also states that "the regulatory body should use the results of the threat assessment as a common basis for determining security requirements for radioactive material and for periodically evaluating their adequacy.

2.4. The sub-sections to follow will address in more detail several issues related to nuclear security threat assessment using a risk-informed-approach, adversaries and their attributes and characteristics, and information security concerns.

RISK INFORMED APPROACH AND THREAT STATEMENTS

2.5. Ref. [1] underscores that an essential element of a nuclear security regime is the use of risk-informed approaches, including in the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth.[2] Taking a risk informed approach to nuclear

[2] The use of a graded approach and defence in depth are discussed in more detail in Ref. [1]

security should involve consideration of: the threat, the attractiveness and vulnerability of potential targets, as well as the potential consequences resulting from malicious acts.

2.6. Ref. [2] recommends that "the State should ensure that the State's physical protection regime is capable of establishing and maintaining the risk of unauthorized removal and sabotage at acceptable levels through risk management." Risk management should include a periodic re-evaluation of the threat and the potential consequences of malicious acts and should ensure that appropriate nuclear security systems and measures are put into place to prevent or acceptably reduce the likelihood of a successful malicious act.

2.7. A nuclear security threat assessment process, for which an overview is provided in Section 3 of this publication and detailed guidance in later chapters, is an evaluation of the existing nuclear security related threats to determine the attributes and characteristics of potential adversaries. This nuclear security threat assessment process makes use of global, regional and domestic sources of information.

2.8. The nuclear security threat assessment process results in the production of a nuclear security threat assessment documentation, from which threat statements can be developed. A threat statement sets out credible adversary attributes and characteristics that activities and facilities associated with nuclear and other radioactive material are to protect against.

2.9. An assessment of the current threat related to nuclear security provided in threat statements such as design basis threats and representative threat statements can be used to facilitate a risk informed approach to nuclear security as well as risk management at individual facilities and activities. Threat statements can assist the design and evaluation of nuclear security systems and measures that take into account the potential consequences of a successful malicious act.

2.10. States could choose to develop two types of threat statements: representative threat statements and/or design basis threats. Representative threat statements are typically used to develop prescriptive regulatory requirements[3] for a certain subset of materials and/or facilities to be protected, while design basis threats are typically defined for specific facilities or

[3] More detailed information on prescriptive and performance-based regulatory approaches can be found in Refs. [2, 3, 8, 9]

activities. For example, a representative threat statement might be used to develop prescriptive regulatory requirements for the protection of Category 1 radioactive sources in use and storage, while a design basis threat might be used to design and evaluate a nuclear security system developed by an operator of a given irradiator using a Category 1 radioactive source to satisfy performance-based requirements to provide effective protection against attack scenarios based on this design basis threat.

2.11. States could choose to define different representative threat statements for: different categories of nuclear and other radioactive materials and different types of facilities and activities (e.g. Category 1 radioactive material, irradiators and transport of radioactive material); different adversary objectives (e.g. theft, sabotage); or cyber specific target assets (e.g. sensitive information, computer based systems for nuclear safety, security, and nuclear material accountancy and control).

2.12. Similarly, States could choose to define design basis threats based on the nuclear security threat assessment documentation that are applicable to specific high risk materials, facilities and/or activities (such as a research reactor, or transport of spent nuclear fuel). These design basis threats would take account of details of the facility or activity such as its design and location, policy considerations like conservatism and public confidence, as well as the missions, capabilities and resources of the regulatory body and the operator.

2.13. Some threats identified during the nuclear security threat assessment process will likely not be included in the design basis threats and representative threat statements. In this case, protection against these threats, even if the operators' nuclear security systems have some inherent protection, need to be considered in the State's contingency plan. Although the State should develop measures to counter these nuclear security related threats, the operator might still have a role in assisting the State either to protect against these nuclear security related threats or to mitigate their consequences.

2.14. Decisions regarding nuclear security risk are ultimately based on current threats of concern to a State, the possibility of new and emerging threats, and decisions regarding how to balance conservatism regarding security with cost and operational impact. The decisions may

also involve considerations such as lessons learned from previous threat assessments, political and economic considerations, and the public's perception of risk..

POTENTIAL ADVERSARIES AND THEIR ATTRIBUTES AND CHARACTERISTICS

2.15. Potential adversaries could include terrorists, criminals, activists and extremists who might seek to acquire and use nuclear or other radioactive material in order to build nuclear explosive devices, radiological dispersal devices or radiation exposure devices. They might also seek to commit sabotage of facilities in which nuclear or other radioactive material is used or stored or to sabotage the transport of such material.

2.16. Adversaries may include insiders, defined as "individual[s] with authorized access to *associated facilities* or *associated activities* or to *sensitive information* or *sensitive information assets*, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities* or *associated activities* or other acts determined by the State to have an adverse impact on nuclear security." [1] Adversaries might seek to acquire authorized access to a facility in order to later function as insiders, or already employed personnel may become insider threats.

2.17. Moreover, the potential for collusion between insiders and external adversaries should be considered. An insider may conduct a criminal or intentional unauthorized act physically or using cyber means at the same time as an external adversary, or the two acts could be sequential.

2.18. There are multiple types of potential criminal or intentional unauthorized acts that adversaries might undertake and that a State should consider. For example, States should consider not only such acts that involve physical access to the facility or activity, but also cyber attacks. Cyber attacks could be aimed at computer-based systems used for nuclear safety (including instrumentation and control systems), nuclear material accountancy and control, and nuclear security. Adversaries might also undertake a blended attack, where an attack on a computer-based system is conducted in combination with criminal or intentional unauthorized act involving access to the facility (such as a physical attack).

2.19. The potential for both insider threats as well as external adversaries to undertake criminal or intentional unauthorized acts resulting in a compromise of the confidentiality, integrity and availability of information contained on computer systems should be considered.

2.20. The potential for stand-off attacks should also be considered. A stand-off attack could involve remote controlled devices operated from a distance such as drones, missiles, sniper rifles or electro-magnetic waves.

2.21. The introduction of malware through the supply chain may be seen as a threat, and could be a result of collusion with cyber threats or of a cyber attack to the supply chain.

2.22. All combinations of possible attacks should be considered: for example, when developing attack scenarios for nuclear security system design, attack scenarios involving collusion between insider threats and external adversaries and using blended cyber-physical attacks should be addressed.

2.23. The relevant attributes and characteristics of a potential adversary describe motivations, intent and capabilities. Motivations could be economic, political, or ideological. Intent may include unauthorized possession of material, radiological sabotage and/or public embarrassment for the operator or the State. The capabilities of an adversary is determined by its composition, including the number of individuals involved, the adversary's organization and coordination, whether insider threats are involved. Capabilities also include the individuals' and organization's abilities, assets and relevant skills, such as tactics, weapons, explosives, transportation, physical and cyber tools, knowledge of software exploits and level of access to the facility or computer systems.

INFORMATION SECURITY CONSIDERATIONS

2.24. All credible information related to threats, including national intelligence and other sensitive information should be used in the development and maintenance of threat statements. Some of this information and many of its sources need to be protected. A design basis threat or a representative threat statement, because of its use in the design and evaluation of nuclear security systems may be protected as sensitive information due to its value to an adversary.

2.25. Detailed guidance on protecting sensitive nuclear security information can be found in Ref. [10].

3. OVERVIEW OF THE PROCESS OF DEVELOPMENT, USE AND MAINTENANCE OF NUCLEAR SECURITY THREAT ASSESSMENT DOCUMENTATION, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

3.1. The process of development, use and maintenance of the nuclear security threat assessment documentation, the design basis threats and representative threat statements consists of five steps:

1. Definition of roles and responsibilities;
2. Performance of the nuclear security threat assessment;
3. Development of design basis threats and representative threat statements;
4. Use of the design basis threats and representative threat statements in the regulatory framework; and
5. Maintenance of nuclear security threat assessment documentation, representative threat statements and design basis threats.

3.2. During Step 1, according to the legal and regulatory framework of the State, the roles and responsibilities in this process should be defined for the State, the regulatory body and other competent authorities, and operators.

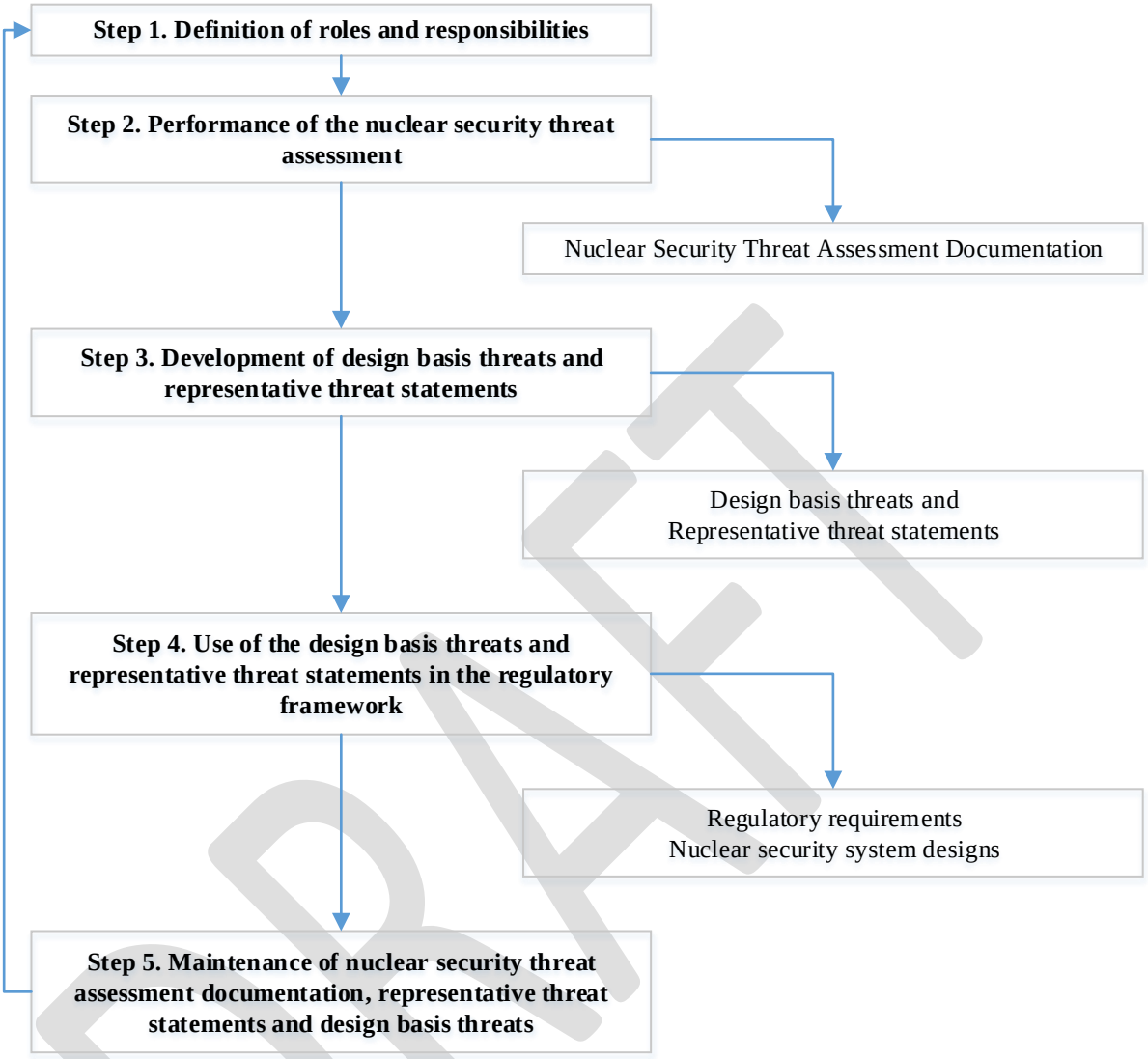

Figure 3.1. Overview of the process

3.3. At Step 2, during the performance of the nuclear security threat assessment, the competent authority responsible for performing the nuclear security threat assessment, together with other relevant competent authorities should collect threat information, including information from open sources, past nuclear security events as well as security events that occurred in non-nuclear related activities. In addition, IAEA databases, especially the Incident and Trafficking Database (ITDB) may be a useful source of threat information. The competent authorities should analyse the collected information and evaluate its potential relevance to nuclear security. The competent authorities should also evaluate the credibility of the threat

information and screen out information that is not credible. Based on this information, they should then identify potential adversaries and likelihoods of adversary actions, attributes and characteristics of the potential adversaries and potential targets. Finally, they should evaluate whether or not specific adversary capabilities are relevant to potential targets, and prepare the nuclear security threat assessment documentation.

3.4. At Step 3, using the nuclear security threat assessment documentation, the competent authority responsible for developing the threat statements - in agreement with other competent authorities, as appropriate - should develop material, facility or activity-specific design basis threats and/or develop representative threat statements applicable to different types, categories of nuclear and other radioactive materials, associated facilities and activities.

3.5. At Step 4, depending on the regulatory approach followed, the regulatory body should take one of two approaches:

(a) Disseminate design basis threats to relevant operators, who should then design their nuclear security systems through the development of facility specific attack scenarios to counter the design basis threats and to meet the security objectives established in the State's legal framework; or

(b) Develop prescriptive regulatory requirements based on the representative threat statements and the security objectives established in the State's legal framework, and ensure that operators implement nuclear security systems and measures in compliance with these requirements.

3.6. At Step 5, the competent authorities should review, and if appropriate revise the nuclear security threat assessment documentation, the design basis threats and the representative threat statements. The determination of whether it is appropriate to revise these documents could be made according to a defined review cycle, in the event of a change in the threat environment, and/or based on lessons learned following a nuclear security event. In the case of new or emerging nuclear security threats requiring immediate consideration, the competent authorities together with the operators, should take the necessary actions to manage these nuclear security threats.

3.7. In Sections 4-8 of this publication, each of these steps will be discussed in more detail, including more specific guidance for States, competent authorities and operators in putting these steps into practice.

4. ROLES AND RESPONSIBILITIES

4.1. The State, the competent authorities, including the regulatory body, and operators have roles and responsibilities related to the nuclear security threat assessment and the development of the design basis threats and/or representative threat statements. These roles and responsibilities should be clearly defined prior to beginning work on the nuclear security threat assessment.

4.2. Guidance on defining these roles and responsibilities is provided in the sub-sections to follow.

STATE

4.3. According to Ref. [1], "The objective of a State's nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event." Later in this publication, it is noted that "Responsibility rests with the State for meeting [this] objective."

4.4. With respect to the nuclear security threat assessment process and development, use and maintenance of the design basis threats and/or representative threat statements, the State is responsible for assigning competent authorities who are leading and participating in

- Performing a nuclear security threat assessment, maintaining a nuclear security threat assessment documentation;
- Developing and maintaining deign basis threats and/or representative threat statements;
- Using the design basis threats and/or representative threat statements[4].

[4] The State may assign different competent authorities to lead the different processes; however, the roles and responsibilities should be clearly defined and the coordination mechanism among competent authorities should be well established.

4.5. The State shall ensure that the hazard assessment, providing basis for a graded approach in preparedness and response for a nuclear or radiological emergency, includes consideration of the results of nuclear security threat assessment [11].

COMPETENT AUTHORITIES

4.6. Competent authorities should be involved in the nuclear security threat assessment process in order to enable the identification of a full range of credible threats to be considered in the nuclear security threat assessment.

4.7. Relevant expertise for gathering and assessing credible threats might exist in several organizations, such as intelligence organizations, a State's ministry of foreign affairs, cyber security centres, law enforcement agencies and military bodies. Such organizations are familiar with the processes of collecting and analysing intelligence information and are skilled in making the necessary judgments. In addition, they may have access to sources of information, including information from international liaisons.

4.8. The responsibilities of competent authorities should include:

(a) Collecting and sharing information on potential threats;

(b) Analysing the available threat information to ensure its credibility;

(c) Developing design basis threats and/or representative threat statements based on the nuclear security threat assessment documentation;

(d)

(e) Coordinating with other competent authorities to determine what subset of credible threats is applicable to nuclear infrastructure;

(f) Maintaining the nuclear security threat assessment documentation, as well as design basis threats and representative threat statements;

(g) Sharing the nuclear security threat assessment documentation, as appropriate, with relevant emergency response organisations;

(h) Considering the nuclear security threat assessment when performing hazard assessment [12].

4.9. A variety of additional competent authorities (for example, the national and local police authorities, armed forces, border control authorities and customs authorities) play a part in protecting against threats related nuclear security, either on their own or in conjunction with others. Moreover, they might have responsibilities for providing support to the operator during a nuclear security event. Such competent authorities should be involved or consulted in the process to develop the design basis threats and representative threat statements, as well as the regulatory requirements.

REGULATORY BODY

4.10. With respect to the nuclear security threat assessment process and development, use and maintenance of the design basis threats and/or representative threat statements, the regulatory body, in coordination with other competent authorities as appropriate, is responsible for:

(a) Developing prescriptive requirements for operators based on the representative threat statements, and/or performance based requirements for and providing the design basis threats to operators to be used for developing attack scenarios and designing nuclear security systems and measures;

(b) Ensuring that operators review appropriately and, as necessary, revise the emergency arrangements taking account of the design basis threats.

OPERATORS

4.11. The operators should implement nuclear security systems and measures that:

(a) meet the regulatory requirements; and/or

(b) protect against a range of facility or activity-specific attack scenarios developed based on the design basis threat.

4.12. The operators' knowledge of the financial, operational and safety impact of specific measures may influence the division of responsibility between the operator and competent authorities for security measures. The operators' input, either formal or informal, should be taken into consideration in developing the design basis threats, representative threat statements and regulatory requirements. Specifically, the operators should provide:

(a) Input on facility and activity specific threats related to nuclear security that should be considered for inclusion in the design basis threats and/or representative threat statements;

(b) Feedback to the regulatory body, as requested, concerning the financial, operational, security and safety impact of potential decisions regarding the design basis threats and/or representative threat statements as well as regulatory requirements; and

(c) Supporting information regarding attack scenarios and adversary attributes and characteristics derived from cyber, physical and blended attacks that may have occurred.

5. PERFORMING A NUCLEAR SECURITY THREAT ASSESSMENT

5.1. The aim of a nuclear security threat assessment is to provide a credible assessment of potential threats, describing the motivations, intentions and capabilities of potential adversaries; however, it is not intended to describe specific attack scenarios.

5.2. A sufficiently detailed and specific description of the potential threat can be used to determine the level of protection that is appropriate and sufficient for nuclear and other radioactive material, associated facilities and activities and provides a basis upon which the nuclear security system can be effectively designed.

5.3. During a nuclear security threat assessment process, information regarding existing or credible potential threats is collected and analysed, and information on threat attributes and characteristics is compiled and aggregated. The output of the nuclear security threat assessment is a detailed description of the threat related to nuclear security referred to as the nuclear security threat assessment documentation. Multiple organizations with different areas of

expertise and responsibility should work closely together to collect and analyse this information, and close working relationships between all relevant organizations are needed for the nuclear security threat assessment to be effective.

5.4. The actions in the process of nuclear security threat assessment are described in detail in the following sub-sections: the collection, analysis of information and intelligence, and the development of the nuclear security threat assessment documentation.

COLLECTION OF RELEVANT THREAT INFORMATION

5.5. As the first action in the nuclear security threat assessment process, a comprehensive collection should be compiled of information and intelligence concerning all potential adversaries as well as their motivations, intentions and capabilities. This information and intelligence can include both sensitive and non-sensitive information, and should address both physical and cyber capabilities of potential insider and external threats.

5.6. To establish this collection, potential sources of information should be identified and relevant information should be collected as well as the sensitivity of the information and needed intelligence that should be considered. If not already in place, a mechanism to share threat information should be established that accounts for the protection of sensitive information. Written agreements or arrangements might be needed to establish relationships for sharing threat information.

5.7. Intelligence and other sources of information related to nuclear security threats might provide sufficient information to design a nuclear security system, however, due to the limitations of intelligence and the dynamic nature of threats, nuclear security systems designed only for the current known threats related to nuclear security may not be effective against future threats.

5.8. The nuclear security threat assessment, as far as possible, should not rely on a single source. The use of intelligence from multiple sources combined into a single coherent assessment will result in the most comprehensive, reliable and robust nuclear security threat assessment. Thus, all credible and relevant national and international sources of information and intelligence should be considered in the collection of data.

5.9. Sources of information and intelligence should include, as appropriate, intelligence organizations, cyber security organizations, law enforcement agencies, INTERPOL, the regulatory body and other competent authorities, customs and border agencies, the military, transportation carriers and shippers, official government reporting from other governmental sources, significant incident reporting by operators, databases maintained by international organizations and open source reporting.

5.10. Domestic and international technical authorities, commercial entities and open databases could also be used as sources of additional information about potential cyber threats. Operators may also have information on cyber threats and their attributes and characteristics that can be used.

5.11. Relevant information regarding adversary attributes and characteristics for analogous high-value, high-consequence critical infrastructure should also be considered.

5.12. Information collected should include details on recent and historical nuclear security events (including those involving computer security), if applicable, and should address the motivation, capability and intent of potential adversaries. Information that may indicate an intent to attack high value or hardened assets and facilities should also be considered, such as evidence of training.

5.13. The information collection action should seek to identify, among others, the following relevant threats:

(a) Global, domestic and local threats;

(b) The potential for physical, cyber and blended attacks; and

(c) Insider threats, external adversaries and threats resulting from collusion of insider threats and external adversaries.

Credible adversary capabilities, even if not yet demonstrated, should also be considered, as well as adversary attack persistence, technological evolution, frequency of attacks, and supply chain concerns (i.e. introducing corrupted hardware and/or software during supply).

ANALYSIS

5.14. Once the collection of relevant threat information is complete, this information should then be organized using information management tools to index and sort it prior to beginning to conduct the analysis. Effectively organizing all available information, including intelligence information, ensures that the needed information is present in the collection and available to be analysed. After the threat information has been organized, it should be analysed to identify and document the credible motives, intentions and capabilities of potential threats related to nuclear security.

5.15. The comprehensiveness of the information collected and the accuracy of the analysis can affect the confidence placed in the design basis threats and representative threat statements resulting from the process.

5.16. Information collection and analysis are continuous, concurrent actions. Analysis will often demonstrate the need for more information and identify previously unknown or emerging threats, leading to a need for further information collection. Analysis of the threat information involves evaluating what is known based on that information, and making a judgment about how adversaries might behave in the future.

5.17. During the analysis process, the credibility of the information used to perform the nuclear security threat assessment should be evaluated. Information provided by law enforcement and intelligence agencies should be accompanied by a judgement on how much confidence can be attached to it. Information derived from sources that are known to have access to the originator of the information and that are judged to be transmitting it accurately and reliably are the most credible. Open source information (e.g. media) should be used only when it is judged to be accurate and factual. The degree of confidence in any information should be taken into account when deciding how that information will be used later. An evaluation of the credibility of information might result in some information being excluded as not relevant to the analysis and might also identify information gaps that should be considered.

5.18. The nuclear security threat assessment process should consider at least the following attributes and characteristics for each identified insider and external threat, although there may not be data available for all the listed attributes and characteristics for each threat:

(a) Motivation, such as political, financial, ideological or personal motivation;

(b) Attack persistence;

(c) Dedication, including level of risk aversion and willingness to put one's own life at risk;

(d) Experience, including the characterization of past nuclear security events that have occurred;

(e) Intentions, such as radiological sabotage of material or of a facility, unauthorized removal of nuclear or other radioactive material, and theft of sensitive information;

(f) Group size, including the attack force, coordination personnel and support personnel;

(g) Weapon types, numbers and availability;

(h) Explosive types, quantities, availability, triggering sophistication, and whether they would be acquired or improvised;

(i) Tools, such as mechanical, thermal, manual, power, electronic, software, electromagnetic and communications equipment;

(j) Modes of transportation, including public, private, land, sea, air, and vehicle type, number, and availability;

(k) Mode of access, both cyber and physical;

(l) Tactics, such as the potential for the use of stealth, deception or force, reconnaissance activities or social engineering;

(m) Planning skills, such as the ability to plan a diversion, adversaries attacking simultaneously in smaller groups, and/or knowledge of the facility layout;

(n) Technical skills, including skills in engineering, use of explosives, chemicals, communications, military or paramilitary experience;

(o) Advanced computer and computer security skills, such as knowledge of: control systems, cyber security, reverse engineering and vulnerability testing of operating systems and applications, hacking communication protocol engineering, vulnerability verification and exploitation techniques, capabilities in creating and maintaining social engineering campaigns, methods and frameworks for source obfuscation, redirection of attribution, networks surveillance and traffic manipulation techniques;

(p) Knowledge, such as target characteristics, site plans and procedures, security plans, security measures, safety measures and radiation protection procedures, operations, potential uses of nuclear or other radioactive material, possible entry points for cyber attacks, vendor support procedures and plans, supply chain and procurement procedures, transportation procedures;

(q) Funding sources, amounts, and availability;

(r) Insider threat concerns, including potential for collusion, passive or active insider involvement, violent or non-violent insider engagement and number of insider threats;

(s) Support structure, such as the presence or absence of local sympathizers, support organizations or logistical support.

In addition to addressing the attributes and characteristics listed, the nuclear security threat assessment should attempt to address the compilation and aggregation of the attributes and characteristics.

OUTPUT: NUCLEAR SECURITY THREAT ASSESSMENT DOCUMENTATION

5.19. The output of the nuclear security threat assessment process is the nuclear security threat assessment documentation, which describes the overall threat environment for nuclear security and all known credible threats that should to be taken into consideration. The supporting

analytical narrative should provide as much detail as possible about these threats and the credibility of the information.

5.20. Both the nuclear security threat assessment documentation and the details of intelligence sources are typically protected as sensitive information.

6. DEVELOPMENT OF DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

6.1. As described in the previous section, the nuclear security threat assessment process results in the production of a nuclear security threat assessment documentation. Using this nuclear security threat assessment documentation as a basis, threat statements that set out credible adversaries that facilities and activities using or storing nuclear or other radioactive material are to protect against, as well as the attributes and characteristics of these adversaries, in the form of either design basis threats or representative threat statements can be developed. Guidance for developing design basis threats and representative threat statements using nuclear security threat assessment documentation is provided in the following sub-sections.

REGULATORY APPROACHES AND THREAT STATEMENTS

6.2. Three different regulatory approaches are possible when regulating an operator: the performance-based approach, the prescriptive approach or the combined approach. In the performance-based approach, the operator should comply with the nuclear security objectives defined by the State taking into account the design basis threat disseminated by the regulatory body. The operator should design and implement a nuclear security system that meets those objectives, achieving a specified level of effectiveness in protecting against malicious acts and providing contingency responses. [8] In the prescriptive approach, the regulatory body establishes requirements for specific nuclear security measures that are necessary to meet the defined nuclear security objectives for each category of nuclear material and each level of potential radiological consequences. These provide a set of ‘baseline’ measures for the operator to implement. [8] The combined approach includes elements from both the prescriptive and

performance-based methods. [8] Further detailed information on each of these regulatory approaches can be found in Ref. [8] and [9].

6.3. As noted in Section 2 of this publication, representative threat statements are typically used to develop prescriptive regulatory requirements for a certain subset of materials, activities and/or facilities to be protected, while design basis threats are typically defined for specific facilities or activities. The regulatory body should adopt the regulatory approach and accompanying choice of representative threat statements or design basis threats that best suits the State's needs and consistent with its legal and regulatory framework. The regulatory body should have its chosen approach approved by the government, since there will likely be resource implications associated with the choice.

6.4. The use of a design basis threat in conjunction with a performance-based regulatory approach as the basis for designing nuclear security systems and measures can lead to an efficient allocation of resources for protection by reducing the uncertainty that might otherwise exist in establishing specific requirements for protection against nuclear security threats. The use of a performance-based approach and a design basis threat not only allows for customization of the design of the nuclear security system to address unique features of the material, activities or facilities (including their industrial and control systems), but also sets a baseline against which the need for modifications in nuclear security systems and measures can be evaluated and provides a clear basis for defining the nuclear security responsibilities of the operator. The use of a design basis threat also provides a more detailed and precise technical basis for design and evaluation criteria and can provide greater assurance that the protection is sufficient.

6.5. However, there are also costs associated with this choice: notably, the use of a design basis threat in conjunction with a performance-based approach means that greater resources and competences will be needed on the part of the regulatory body and the operator. The decision to pursue a design basis threat may be influenced by the limited availability of the necessary capabilities and resources in the regulatory body for defining and at the operator level for effectively using a design basis threat to design security systems and measures. However, if the criteria discussed in the following paragraph suggest that the level of assurance

associated with a design basis threat is needed, the State should seek to make the necessary resources and capabilities available.

6.6. States should consider using the following criteria to determine whether or not to use a design basis threat. First, the State's physical protection requirements for nuclear material and nuclear facilities should be based on a design basis threat specifically for unauthorized removal of Category I nuclear material and sabotage of nuclear material and nuclear facilities that has potentially high radiological consequences [2]. A State should also consider the development of a design basis threat if it has determined that the potential consequences of a malicious act would be severe.

6.7. Development of a design basis threat should be considered for protection of assets with which lesser consequences are associated if:

(a) The nuclear security threat assessment documentation indicates the existence of a threat with known intent to commit a malicious act affecting the asset under consideration;

(b) The nuclear security threat assessment documentation indicates a highly capable threat for which intent is unknown; or

(c) There is too much uncertainty in the nuclear security threat assessment owing to a limited amount of data or a low level of confidence in the sources of the data.

6.8. For new facilities, a State may wish to consider the possible long-term advantages of designing protection against more conservative threat attributes and characteristics, given the cost implications of upgrades added after the facility is in operation.

6.9. Regardless of whether a design basis threat in conjunction with a performance based regulatory approach is used, or a representative threat statement in conjunction with a prescriptive regulatory approach, a threat related basis should be used to design security systems and measures for nuclear and other radioactive material, associated facilities and activities.

DEVELOPING A DESIGN BASIS THREAT

6.10. A design basis threat should be developed from the nuclear security threat assessment documentation using a process consisting of five actions:

1. Screening of the nuclear threat assessment documentation for relevant nuclear security threats with motivation, intention and/or capability to commit a malicious act;
2. Collating adversary attributes and characteristics;
3. Modifying collated adversary attributes and characteristics on the basis of relevant policy considerations;
4. Tailoring adversary attributes and characteristics to a specific facility, activity; and
5. Finalization of the design basis threat.

6.11. Using the nuclear security threat assessment documentation as a basis for the design basis threat helps to ensure that the resulting design basis threat is realistic and credible.

Screening the nuclear security threat assessment documentation

6.12. First of all, the targets that could be associated with unacceptable consequences, as defined by the State, as a result of malicious acts, should be identified. These targets should then be considered in conjunction with the attributes and characteristics of the postulated adversaries described in the nuclear security threat assessment document in order to determine threats that are relevant to the targets and may cause unacceptable consequences. This consideration should include a review of the capabilities, motivations and intentions of the postulated adversaries with respect to these targets.

6.13. The adversaries described in the nuclear security threat assessment document should be reviewed to determine whether or not they possess the capabilities necessary to commit a malicious act that could lead to unacceptable consequences. If the capabilities of a given adversary are not sufficient to commit an act that could lead to unacceptable consequences, then that adversary should be excluded from further consideration; however, considerable

caution should be exercised when making this decision. Notably, a nuclear security threat should not be excluded from further consideration on the basis that the existing nuclear security system in place to protect a facility or activity is sufficient to repel the adversary. In fact, existing nuclear security measures can be ignored during the development of a design basis threat[5].

6.14. After the review of capabilities, each adversary is further reviewed to determine if, in addition to having sufficient capabilities to commit a malicious act, it is also believed to have sufficient motivation or the intent to commit such an act. If neither sufficient motivation nor intent is determined to be present, the adversary might be excluded from further consideration; however, care must be exercised when excluding a highly capable threat solely on the basis of perceived lack of motivation or intent. The regulatory body should determine whether or not the adversary's perceived motivation is inconsistent with the consequences of such a malicious act and whether the degree of confidence in the data used to assess its motivation and intent is sufficient. The decision to exclude the adversary should then be based on these factors.

6.15. The reasons for the exclusion of any adversary present in the nuclear security threat assessment documentation from further consideration for the design basis threat should be well documented. Any adversary excluded from consideration should be considered again if new information changing the reasons for the exclusion is acquired at a later time.

6.16. At the end of the screening process, a list of all credible adversaries that are capable and may be motivated or may have the intention to commit a malicious act leading to unacceptable consequences should be produced.

Collating adversary attributes and characteristics

6.17. Each of the various relevant adversaries identified in the nuclear security threat assessment should be associated with an appropriate adversary type (e.g. terrorists, criminals, activists or extremists) to be described in the design basis threat and credible adversary descriptions should be developed. The threat meant by an adversary type in the design basis

[5] These nuclear security measures might later be removed by an operator, if the design basis threat does not include threat attributes and characteristics against which they would be effective and needed.

threat should represent the range of adversary attributes and characteristics belonging to those adversaries associated with the adversary type.

6.18. The relevant adversary attributes and characteristics associated with a given adversary type should be collated. The collated adversary attributes and characteristics should not simply represent a combination of the most extreme attributes and characteristics of each relevant adversary as this may result in an unrealistic definition of the adversary. In fact, some of these attributes and characteristics may even be mutually incompatible.

Modifying collated adversary attributes and characteristics to account for policy factors

6.19. The collated adversary attributes and characteristics should be assessed in light of the degree of conservatism desired in the nuclear security threat assessment, the cost-benefit-consequence trade-offs that need to be made, and other policy factors identified. This may result in adjustments to the collated adversary attributes and characteristics in order to enable a sustainable level of security, and may result in a change in the level of adversary capabilities.

6.20. First, the collated adversary attributes and characteristics may be adjusted to accommodate the degree of conservatism desired in the nuclear security threat assessment. For example, they may be adjusted to compensate for uncertainty and different interpretations in the data used in the nuclear security threat assessment; to ensure the effectiveness of the operators' nuclear security systems and measures as the nuclear security threat evolves with time; or to include attributes and characteristics of potential threats about which there is no current intelligence because it is prudent to do so.

6.21. In addition, cost–benefit–consequence trade-offs should be accounted for in the definition of the collated adversary attributes and characteristics. This includes balancing the benefit to society of the assets, the consequences for society of successful malicious acts against the assets, and the costs to society of reducing the risks of such acts and implementing appropriate nuclear security measures comparable with that for other assets and infrastructure of similar consequence severity, such as protection for explosives, chemicals, and biological agents.

6.22. Other policy factors may also need to be accounted for, such as the division of nuclear security responsibilities between the State and operators; the impact of decisions made regarding risk acceptance on public confidence; the contribution to public welfare of the assets (e.g. nuclear or radioactive material) being protected; the confidence of neighbouring States in a State's nuclear security; and ongoing threat situations in neighbouring States.

6.23. Conservatism and the other policy factors noted here are likely to result in an increase in the capability level of collated adversary attributes and characteristics in the design basis threat, whereas cost–benefit trade-offs will likely decrease them.

Tailoring adversary attributes and characteristics to specific facilities and activities

6.24. Once the representative adversary attributes and characteristics have been broadly defined, they may be tailored to specific facilities and activities. For facilities, site location and accessibility, specific design features of the facility, the operating practices at the facility and local threats could be considered. For activities, operating practices, the mode and route of transport, as well as specific local threats could be considered.

Finalization of the design basis threat

6.25. Prior to using a design basis threat in the regulatory framework, the comments from other competent authorities and affected parties should be considered. The final decision on the content of a design basis threat and the responsibility for this content, should rest with the competent authority assigned to lead the development process by the State.

6.26. A model of a design basis threat is provided as Annex 1.

DEVELOPING A REPRESENTATIVE THREAT STATEMENT

6.27. As with a design basis threat, a representative threat statement should also be developed based on the nuclear security threat assessment documentation. The development process of a representative threat statement follows the approach described for a design basis threat, but is typically less rigorous at each stage, and the process of the development of a representative

threat statement might involve fewer organizations. Moreover, adversary attributes and characteristics are not tailored to a specific facility or activity.

6.28. The process of development of a representative threat statement should include the following four steps:

1. Screening the nuclear security threat assessment documentation to identify adversaries that possess the capabilities necessary to commit a malicious act that could lead to unacceptable consequences as well as the motivation or intent to do so;

2. Grouping of attributes and characteristics of adversaries into sets of representative adversary attributes and characteristics;

3. Modification of representative adversary attributes and characteristics based on policy factors; and

4. Finalization of the representative threat statement.

THREATS WITHIN AND BEYOND THE DESIGN BASIS THREAT

6.29. During the nuclear security threat assessment process, a broad range of adversary threat capabilities are likely to be identified, ranging from adversaries with low threat capabilities to those with high threat capabilities. For this reason, accounting for current known, actual and prevailing threats, the State will likely need to determine a boundary threat capability level above which threat capabilities are determined to be so high that it would not be appropriate to use these threat capabilities as a basis for design requirements for nuclear security systems and measures, and thus they would not be appropriate for use in a threat statement.

6.30. The design basis threats and representative threat statements should then be based on adversaries with capabilities that fall below this cutoff, with the implication that the operator does not have prime responsibility for protection against adversaries with higher capabilities. Because the overall responsibility for nuclear security rests with the State, responsibility for countering adversaries with capabilities above this cutoff level will rest primarily with the State. This is a decision regarding the appropriate level of nuclear security risk to protect

against, and the determination will need to balance cost, operational impact and other considerations.

7. USE OF DESIGN BASIS THREAT AND REPRESENTATIVE THREAT STATEMENTS

7.1. As discussed at the beginning of Section 6, a State may choose to use a performance-based regulatory approach, a prescriptive regulatory approach, or a combined approach. The use of design basis threats and representative threat statements in each of these regulatory approaches is discussed in the sub-sections to follow.

PERFORMANCE BASED REGULATORY APPROACH

7.2. In a performance based regulatory approach, the design basis threat and the State's nuclear security objectives provide the basis for designing, implementing and evaluating nuclear security systems and measures.

7.3. A process for using design basis threats as part of a performance-based regulatory approach includes:

(a) The regulatory body should disseminate the design basis threats to the operators;

(b) Each operator should identify targets within its own facilities and/or activities, then, in coordination with the regulatory body, should develop attack scenarios based on the design basis threats provided;

(c) The operators should design nuclear security systems and measures to address adversaries with the attributes and characteristics described in the design basis threat;

(d) Each operator should describe its nuclear security system design in the security plan and submit this plan to the regulatory body for approval, if required;

(e) The regulatory body should evaluate the effectiveness of the operator's nuclear security system design, based on the submitted security plan. If the results of this evaluation indicate that an operator's planned nuclear security system would not be effective to protect against the attack scenarios developed by the operator at step (b), the regulatory body should require the operator redesign the system to address any identified deficiencies;

(f) When the security plan is approved, the operator should put its nuclear security system and measures in place according to this plan.

7.4. Relevant emergency response organizations including the regulatory body and the operator should use the results of the nuclear security threat assessment in the hazard assessment to allow for adequate emergency arrangements to be established for preparedness and response for a nuclear or radiological emergency triggered by a nuclear security event and for a coordinated and integrated response.

PRESCRIPTIVE REGULATORY APPROACH

7.5. In a prescriptive regulatory approach, the representative threat statements appropriate to the category of material, type of facility or activity should be used by the regulatory body to develop prescriptive regulatory requirements, taking account of nuclear security objectives defined by the State. The prescriptive regulatory requirements should specify required nuclear security systems and measures that, if implemented, would ensure sufficient protection to meet the objectives of the State's nuclear security regime. Guidance that could assist States in developing such prescriptive regulatory requirements can be found in Refs. [4, 5, 8, 9 and 10].

7.6. A process for using representative threat statements as part of a prescriptive regulatory approach includes:

(a) The regulatory body should develop attack scenarios based on each representative threat statement and design model nuclear security systems and measures for different category of materials, type of facilities and activities;

(b) The regulatory body should consider the recommendations and guidance in relevant IAEA NSS publications such as Refs. [4, 5, 8, 9 and 10], as appropriate, and determine whether or not these measures are sufficient for meeting nuclear security objectives or if additional security measures would need to be added to protect against the relevant representative threat statement;

(c) The regulatory body, should develop prescriptive regulatory requirements for nuclear security systems and measures, taking account of the model nuclear security measures developed;

(d) The operators should implement the nuclear security measures as prescribed by the relevant regulatory requirements.

COMBINED APPROACH

7.7. As noted in Section 2 and in Refs. [8 and 9], elements of both prescriptive and performance based approaches used in a combined regulatory approach.

7.8. The State might apply a performance-based approach for facilities and activities where the benefit outweighs the cost. For example, the State might decide to apply a performance-based approach to certain material, facilities and activities for which greater assurance is appropriate due to the potential consequences that could result from a nuclear security event at these locations. The State may decide to concurrently apply a prescriptive approach to material, facilities and activities where a nuclear security event would result in less severe potential consequences. The State may decide as well that some threats should be addressed with a performance based approach while others are addressed with a prescriptive approach.

DEVELOPING ATTACK SCENARIOS

7.9. The development of attack scenarios relies on an understanding of how adversary attributes and characteristics might be used to carry out a malicious act, as well as of whether and how different adversaries would interact to carry out such an act.

7.10. The attack scenario is a postulated or assumed set of conditions and/or events. Attack scenarios are most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as a possible nuclear security event. An attack scenario might represent the conditions at a single point in time or a single event, or could comprise a history over time of conditions and/or events (including processes) leading to and/or following from a nuclear security event, including potential delayed impacts.

7.11. Attack scenarios should consider all credible combinations of adversary attributes and characteristics defined in a representative threat statement or a design basis threat, including collusion between insiders and external adversaries and combinations of physical and cyber attributes and characteristics, and likely adversary pathways, time and approaches of penetration based on defeat methods and delay times of physical and cyber barriers, as well as defeat methods and detection probabilities of sensors and cyber monitoring.

7.12. In particular, cyber involvement in scenarios should be considered. While a cyber attack alone will most likely not lead to unauthorized removal of material, a cyber attack can support the compromise of nuclear security measures that deter, detect, delay and respond to an attack. A cyber attack might also be used to reduce the effectiveness of the technology needed to prevent and detect an attack. A cyber attack might also result in degradation of important safety, security, nuclear material accounting and control, or emergency preparedness and response functions which may lead to sabotage success or provide conditions for successful completion of an attack intended to sabotage equipment.

7.13. The restrictions for feasibility of an attack scenario are its complexity, including factors such as the total weight and capabilities of adversary tools needed, the ability of adversaries to hide tools at access control points, the total number of external adversaries, the realism of adversary and defender physical capabilities, the number of insider threats involved and the extent of their collusion, the capability of physical barriers, and the capability of detection technology and cyber monitoring.

8. MAINTENANCE AND REVIEW OF NUCLEAR SECURITY THREAT ASSESSMENT DOCUMENTATION AND THREAT STATEMENTS

8.1. The the nuclear security threat assessment documentation should be periodically reviewed in order to assess if it still presents a comprehensive and properly balanced view of the credible threat to nuclear security in the State.

8.2. Design basis threats and representative threat statements may also need to be reviewed due to changes in policy considerations and/or based on experience gained during the design and evaluation of nuclear security systems and measures.

8.3. Consideration of new and evolving threat capabilities not known to be directly related to nuclear security could be incorporated in the review of the nuclear security threat assessment document to determine any possible relevance or impact these threats may have on nuclear and other radioactive material, associated facilities and activities.

8.4. The periodic review of the nuclear security threat assessment documentation, design basis threats and representative threat statements might be initiated, for example, on a yearly basis. The periodic review should follow the same process as that used to perform the nuclear security threat assessment, and new design basis threats and representative threat statements should be developed, if appropriate.

8.5. A number of events may lead to a need for a review of the nuclear security assessment documentation outside the periodic review process. The conditions or events might trigger such a review, including:

(a) An event or act, internal or external to the State, on State level or in connection with nuclear and other radioactive associated facilities and activities that significantly changes the perception of or actual level of the threat;

(b) Significant changes in government policy, law or international arrangements that affect the responsibility of the State authorities or the operator, for example, changes involving the use of deadly force, response arrangements or organizational responsibilities;

(c) Changes in activities or facilities associated with nuclear and other radioactive material that could introduce new or exclude potential consequences, such as construction of a different type of facility, use of material of higher enrichment, a new practice for the use of nuclear or other radioactive material, or repatriation of high enriched uranium, operation with lower category material, nuclear safety improvements;

(d) A proposal for review by a competent authority, organization or operator.

8.6. A review will not necessarily result in revision of the nuclear security threat assessment documentation, the design basis threats or representative threat statements. However, if the review shows that the nuclear security threat assessment documentation does not adequately consider all credible threats, including new and emerging threats, the threat assessment documentation should be revised with the involvement of all relevant organizations. If there are substantial and fundamental changes in the nuclear security threat assessment documentation, the design basis threats and representative threat statements should also be revised.

RESPONDING TO NEW AND EMERGING THREATS

8.7. Situations may arise outside of the regular review process in which adversaries are demonstrated to or suspected to possess unexpected physical or cyber attributes that are threatening enough to need immediate action on the part of the State. Information and intelligence may become available on these matters through both official and informal channels.

8.8. In addition to the process of developing and maintaining design basis threats and representative threat statements, the regulatory body and the competent authorities should put a process in place for the sharing of threat information among the competent authorities and with relevant operators.

8.9. If an operator receives information on such a change in the threat through informal channels, the operator should inform the regulatory body and other competent authorities as appropriate, in order to assess credibility, applicability and severity of the potential impact of this change in the threat and to determine how and how urgently the operator needs to respond.

8.10. Establishing a system of pre-determined levels of elevated threat and corresponding pre-determined sets of additional nuclear security measures to be implemented by operators at each level of elevated threat can be used to provide sufficient protection in such situations.

9. REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIR/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G

[6] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).

[7] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016)

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018). [TO BE PUBLISHED]

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standard Series, No. GSR Part 7

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standard Series, No. GS-G-2.1

[13]

APPENDIX

A MODEL DESIGN BASIS THREAT

	Armed	Unarmed
Action		
Theft[6]	Insert yes or no	Insert yes or no
Sabotage[7]	Insert yes or no	Insert yes or no
Common attributes and characteristics		
Number	Insert a number	Insert a number
Level of funding	Insert low or high	Insert low or high
Insider support	Insert active or passive, and violent or non-violent	Insert active or passive, and violent or non-violent
Tactics	Insert stealth or force	Insert stealth or force
Planning skills	Insert ability to plan a diversion, and/or adversaries attacking simultaneously in smaller groups, and/or knowledge on the facility layout	Insert ability to plan a diversion, and/or adversaries attacking simultaneously in smaller groups, and/or knowledge on the facility layout
Physical attributes and characteristics		
Willingness to kill	Insert yes or no	Insert yes or no
Willingness to die	Insert yes or no	Insert yes or no
Pathway	Insert air, road, rail, water, and/or underground	Insert air, road, rail, water, and/or underground
Type of weapons	Insert automatic weapons, semiautomatic weapons, side arms, and/or knives	Not Applicable
Explosive	Insert the type and quantity of explosive	Not Applicable
Tools	Insert power tools, hand tools, and/or tools available on-site	Insert power tools, hand tools, and/or tools available on-site
Technical skills	Insert sophisticated explosive breaching, disabling communications lines, and/or operating facility equipment	Insert sophisticated explosive breaching, disabling communications lines, and/or operating facility equipment

[6] May add criteria for the amount of material removed, and/or one-time or protracted theft

[7] May add criteria for radiological consequences

Contributing insider	Insert security guard, technical maintenance of equipment, and/or material handler	Insert security guard, technical maintenance of equipment, and/or material handler
Cyber attributes and characteristics		
Software tools	Insert standard software tools, malware tools, and/or own developed tools	Insert standard software tools, malware tools, and/or own developed tools
Expertise	Insert social engineering, using commercial tools, develop new software tools; office domain, process control domain, and/or knowledge about the applied IT system	Insert social engineering, using commercial tools, develop new software tools; office domain, process control domain, and/or knowledge about the applied IT system
Hardware tools	Insert notebook, mobile phone, connection to cables, and/or routers	Insert notebook, mobile phone, connection to cables, and/or routers
Ability to influence the supply chain	Insert yes/no	Insert yes/no
Attack persistence	Insert long term, and/or repeated attacking capability	Insert long term, and/or repeated attacking capability
Contributing insider	Insert access authorization, control the processes in I&C systems by normal user, administrator, and/or third party vendor	Insert access authorization, control the processes in I&C systems by normal user, administrator, and/or third party vendor

1