SECURITY FOR NEW REACTORS

TRAVIS RYAN LEACH
United States Nuclear Regulatory Commission
Rockville, Maryland, United States
Email: travis.leach@nrc.gov

Security for New Reactors

The U.S. Nuclear Regulatory Commission (NRC) has a strong and robust security regulatory framework, which contains both performance-based and prescriptive requirements. That framework was designed with traditional large light water reactors in mind. The NRC staff anticipates that new reactor applicants and licensees will consider safety and security requirements early in the design process, such that they will effectively resolve security challenges through facility design, engineered security features, and mitigation measures with little or no reliance on human actions. This design approach may make the existing framework overly burdensome based on the risk of the facility. The NRC is considering whether to add alternative physical security requirements for small modular and advanced reactor applicants and licensees to its existing security framework. Separately, the agency is proposing to add a new part to its regulations that would establish an optional, risk-informed, technology-inclusive framework for new commercial nuclear power plants (NPPs). Both proposed rulemakings contain voluntary measures and risk-informed approaches to address a comprehensive range of security disciplines, including physical security, cybersecurity, fitness for duty, and access authorization, that may be used by an applicant based on the results of a radiological consequence analysis. The paper provides an overview of NRC's proposed changes to its existing physical security regulatory framework to better accommodate new NPP facilities.

1. INTRODUCTION

Currently, an NPP applicant must be licensed under Title 10 of the *Code of Federal Regulations* (10 CFR), Part 50, "Domestic Licensing of Production and Utilization Facilities," or Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Both 10 CFR Part 50 and 52 require a licensee to meet the security requirements in 10 CFR Part 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." These regulations were developed considering the current fleet of large light water reactors (LWR). As early as 2008, the NRC issued a policy statement on advanced reactors which states, in part, that the design of advanced reactors should "include considerations for safety and security requirements together in the design process such that security issues (e.g., newly identified threats of terrorist attacks) can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with reduced reliance on human actions." (Federal Register, Volume 73, page 60612) As the nuclear industry is exploring and embracing new reactor designs, the NRC is developing proposed rulemakings to consider the technological advancements associated with those designs.

New reactor technology introduces key features that need to be considered from a physical protection perspective. Some of those features may reduce the need for traditional security measures, such as passive safety features, lower offsite dose consequences, and below-grade facility construction. Other aspects, such as the use of a more highly enriched fuel, the potential for diverse locations of irradiated fuel on sites, and the ability to control a reactor remotely, may require new reactor owners or operators to consider different security challenges than those contemplated for the LWRs operating today. The use of security-by-design approaches provides a unique opportunity to design an inherently more secure reactor and facility than exists for the current domestic fleet of LWRs, most of which had security features added after they were constructed. Designers are incorporating physical security features into certain designs, including new and evolving technologies for intrusion detection and assessment; hardening interior and exterior walls; locating critical structures, systems, and components below ground; and minimizing access points to vital equipment and operations areas.

In January 2019, President Trump signed the Nuclear Energy Innovation and Modernization Act (NEIMA) into law. This law directed the NRC to "…complete a rulemaking to establish a technology-inclusive, regulatory framework for optional use by commercial advanced nuclear reactor applicants for new reactor license applications" by December 31, 2027 (Public Law No. 115-439, issued January 14, 2019). The paper summarizes the NRC's existing framework for licensing and regulating security under 10 CFR Parts 50 and 52; discusses a

preliminary proposed rule, "Alternative Physical Security Requirements for Advanced Reactors," referred to as the "limited-scope rule," which would allow small modular reactors (SMR) and advanced reactor applicants to implement up to four physical security alternative approaches; and explores the NEIMA-directed "Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," rulemaking, which would create a voluntary framework for all new reactor applicants in a new 10 CFR Part 53.

2. EXISTING SECURITY FRAMEWORK

Existing NRC security regulations contain performance-based and prescriptive security requirements that require NPP licensees to establish, implement, and maintain physical protection programs that defend against the design basis threat (DBT) of radiological sabotage, and prevent significant core damage and spent fuel sabotage. The NRC has established two DBTs in 10 CFR 73.1, "Purpose and scope": the DBT of radiological sabotage and the DBT of theft or diversion of formula quantities of strategic special nuclear material. These Commission-approved DBTs are based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups and organizations. The DBTs describe the threat and adversary force that NRC licensees and their private security forces can reasonably be expected to defend against. Commercial NPP licensees are required to protect against the DBT of radiological sabotage.

The performance objective in the existing security framework is for NPP licensees to implement physical protection programs that provide high assurance[1] that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. The requirements in the regulations provide reasonable assurance that NPP licensees will detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage using effective security organizations and Commission-approved security plans that address significant security elements, including physical barriers; target sets; access controls; search programs; detection and assessment systems; communications; security response; maintenance, testing, and calibration of security equipment; and compensatory measures.

2.1 Physical barriers

Physical barriers must meet the definition of a physical barrier and the associated requirements in the regulations. There are different types of physical barriers that NPP licensees use throughout the different layers of their sites: owner-controlled areas, protected areas, and vital areas. Physical barriers can serve one or more functions. Two common functions for physical barriers are 1) delaying an adversary by increasing the time it takes the adversary to reach its objective(s), and 2) channelling an adversary into areas of a site where a licensee's physical protection program or protective strategy is strongest. The NRC's existing security framework has prescriptive requirements for some physical barriers, such as fences and structural elements like walls, floors, and ceilings, and performance-based requirements for other types of barriers, such as jersey barriers and bollards.

2.2 Access controls

The NRC requires licensees to establish, implement, and maintain access control procedures for each barrier, when necessary, to ensure only authorized personnel, vehicles, and materials are permitted past a barrier. Access controls involve measures to regulate and monitor entry into sensitive areas within NPP facilities, and they are essential for preventing unauthorized access, safeguarding nuclear materials, and protecting against radiological sabotage. Key components of licensees' access control programs include the tools and equipment (e.g., ID badges, biometric scanners, access codes) that licensees use to identify, verify, and search individuals

[1] The Commission stated in staff requirements memorandum (SRM) "SRM-SECY-16-0073 – Options and Recommendations for the Force-On-Force Inspection Program in Response to SRM-SECY-14-0088," issued October 5, 2016, that "the concept of 'high assurance' of adequate protection found in the NRC security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate." The Commission reiterated this point in "SRM-SECY-18-0076 – Options and Recommendation for Physical Security for Advanced Reactors," issued November 19, 2018.

who have unescorted access to site's protected areas. Licensees are also required to have procedures for screening and monitoring visitors, which typically involve assigning escorts to maintain control of visitors while onsite.

2.3 Search programs

The objective of NPP licensees' search programs is to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, and other items that a DBT adversary could use to commit radiological sabotage. When licensees develop their search programs, they consider the design and layout of access portals, search areas, and equipment to ensure that search personnel have the optimum oversight, observation, and control of each person, vehicle, and package proceeding through the search process. With limited exceptions, the NRC requires NPP licensees to search all personnel, vehicles, and materials before they enter facilities' protected areas. Licensees determine how they will perform the protected area searches and whether they may also need to search personnel, vehicles, or materials at other locations on their facilities (e.g., prior to entering an owner-controlled area) to adequately defend against the DBT. When searches are necessary, trained and qualified personnel perform the required physical or electronic examinations, inspections, or checks to ensure that only authorized people, vehicles, and materials are allowed to proceed past the associated barrier(s) and into a designated area.

2.4 Detection and assessment systems

Detection and assessment systems are critical elements of licensees' physical protection programs because they provide the foundation for security response. Detection equipment provides licensees with indications that threats may be present, and assessment systems enable licensees to identify the potential threats and quickly determine the actions needed to resolve situations that pose a challenge to physical security. Detection systems include various types of sensors that can detect unauthorized presences or intrusion attempts, such as motion sensors, surveillance cameras, access control systems, and perimeter intrusion detection systems. Assessment systems enable licensees to identify and evaluate the significance of detected events and may include cameras, video capture systems, computerized monitoring or analysis systems, and site procedures. The NRC requires NPP licensees to monitor required detection and assessment systems with two onsite alarm stations, each of which is continuously staffed with a trained and qualified alarm station operator and can perform the following five activities: 1) receive and monitor signals for intrusion detection, 2) receive and monitor video image signals to assess intrusion, 3) communicate with onsite security to assist with implementing a security response, 4) provide command and control, and 5) summon offsite assistance. Operating NPP licensees are permitted to protect their two alarm stations differently, but new reactor applicants seeking a license would be required to protect both alarm stations to a more stringent standard.

2.5 Communication capabilities

The NRC requires NPP licensees to have effective and continuous communications with onsite and offsite resources to ensure effective security operations, response, and command and control during normal and emergency situations. To address the DBT adversary's capability to interfere or inhibit radio communications, licensees' internal communication systems must consist of primary and alternate capabilities to ensure they have reliable systems for communicating among security personnel, security and plant management, and other relevant site departments. Examples of internal communications systems may include telephone or other hardwired systems, two-way radios, duress alarms, and intercoms. External communications enable licensees to notify offsite entities, such as law enforcement, fire or medical response organizations, and regulatory authorities to effectively integrate responding offsite resources into licensee responses.

2.6 Response requirements

NRC response requirements specify the actions that NPP licensees must take to ensure that armed response personnel are properly trained, qualified, and equipped to implement the sites' protective strategies. For example, an NPP licensee is required to maintain, at all times, a security organization that includes at least 10 armed responders who are located inside a site's protected area and whose sole responsibility is to be immediately

available to interdict and neutralize threats up to and including the DBT. The licensee must train its armed responders to know and understand critical protective strategy elements, including a facility's target sets and protective strategy, and the armed responders' specific roles and timelines for implementing the strategy. Licensees evaluate their armed responders' capabilities by conducting tactical response drills at least once every three months and force-on-force exercises at least once per year.

2.7 Equipment maintenance, testing, and calibration

Licensees are required to establish and implement maintenance, testing, and calibration programs that ensure sites' security systems and equipment are tested for operability and performance at predetermined intervals, maintained in an operable condition, and available and capable of performing their intended functions. Examples of security system equipment that licensees maintain under such programs are secondary and uninterruptible power supplies, intrusion detection systems, access controls, and communication devices. Maintenance activities help to maximize availability and maintain the integrity of security systems; regular testing verifies the performance and functionality of security equipment to ensure it operates as intended; and calibration ensures such equipment is accurate and reliable.

2.8 Compensatory measures

Compensatory measures are additional security measures that NPP licensees are required to implement when normal physical protection capabilities (e.g., security personnel, equipment, systems, components, procedures) are degraded or inoperable. In such situations, licensees must 1) implement compensatory measures within the specific timeframes necessary to ensure that the degraded or inoperable condition has not been, and cannot be, exploited; and 2) ensure that the implemented compensatory measures provide a level of protection that is at least equivalent to the normal measure(s) for which they are substituting. Examples of security compensatory measures include increased security patrols, temporary physical barriers to restrict access, temporary relocation or protection of target set elements or other critical assets, manually processing personnel entering or exiting a protected area, and continuous human monitoring of a perimeter alarm zone.

2.9 Exemptions and alternative measures

NPP licensees may decide that they cannot or will not meet one or more of the NRC's physical security requirements and request an exemption, or they may want to use a method(s) to meet a security requirement(s) that is different from the measure(s) that NRC's regulations prescribe and request approval of an alternative. In either case, a licensee is required to obtain approval from the NRC before deviating from the regulations. A licensee requesting an exemption(s) to a physical security requirement(s) would describe in its application the exemption(s) it is seeking, why it is seeking the exemption(s), the applicable regulatory requirement(s), and whether the requested exemption(s) is/are temporary or permanent. Additionally, the licensee would need to demonstrate that the requested exemption(s) is/are authorized by law; would not endanger life, property or the common defense and security; and would otherwise be in the public interest. A licensee requesting to use an alternative measure(s) to meet a physical security requirement would 1) describe the desired changes, 2) demonstrate that the proposed alternative security measure would meet the same performance objective(s) and requirement(s) as the prescribe measure(s), and 3) provide a basis for each proposed alternative measure that demonstrates how the measure would provide a level of protection at least equivalent to the protection provided by the prescribed measure(s). Either process can take a year or longer to complete, barring exigent circumstances.

3. PROPOSED LIMITED-SCOPE RULE

Although the existing security framework is adequate for licensing and regulating new reactors, the NRC staff developed the proposed limited-scope rule, "Proposed Rule: Alternative Physical Security Requirements for Advanced Reactors," to 1) consider the reduced risk that may be posed by a new reactor design and 2) avoid the need for new reactor applicants to submit, on a case-by-case basis, applications for exemptions or alternative measures to existing security requirements because they intend to use certain specific approaches that differ from

the existing requirements. The proposed limited-scope rule would continue to ensure that licensees' physical protection programs adequately protect against the DBT of radiological sabotage. Advanced reactors or SMRs that meet the proposed eligibility requirements and elect to implement one or more of the proposed alternative physical security requirements would still be required to meet the other physical security requirements in the NRC security requirements for nuclear power reactors.

The proposed limited-scope rule would create a new subsection in the existing security framework. Under this new subsection, a new reactor applicant or licensee would need to satisfy two primary elements before it would be eligible to implement any of the alternative physical security requirements in the proposed limited-scope rule. The first element would be that the new reactor applicant or licensee would need to be operating a reactor design that meets the definition of an SMR or an advanced reactor (i.e., non-LWR). The second element would be that the new reactor applicant or licensee would need to demonstrate that the consequences of a postulated radiological release that would result from a postulated DBT-initiated event would not exceed the offsite dose reference values defined in the current regulations governing nuclear power reactor licensing.

When performing the technical analysis to demonstrate the consequences of a postulated radiological release that results from a postulated security-initiated event, SMR and non-LWR applicants and licensees would be permitted to consider a limited number of physical security features. Examples of the features that could be considered are security-related features that could be activated or initiated from a reactor control room and passive security features. Passive security features include security doors that are normally locked, welded, pinned, or otherwise secured; security fencing with access points that are normally kept in the denial position (e.g., gates that are closed and locked); and permanently installed vehicle barrier system(s) with an active barrier(s) that is normally kept in the denial position.

Importantly, under the limited-scope rule, demonstrating that potential offsite consequences would not exceed the dose reference values would not relieve an SMR or non-LWR applicant or licensee from the responsibility to defend against the DBT. Rather, the applicant or licensee would be permitted to implement any or all of four proposed alternative physical security requirements: 1) relying on fewer than 10 armed responders to interdict and neutralize the DBT adversary, 2) relying on law enforcement or other offsite responders to interdict and neutralize the DBT adversary, 3) employing measures other than physical barriers to provide delay or deny access to a DBT adversary, and 4) employing an offsite secondary alarm station. On February 2, 2024, the NRC released preliminary Draft Regulatory Guide, DG-5072, "Guidance for Alternative Physical Security Requirements for Small Modular Reactors and Non-Light Water Reactors," for public awareness. DG-5072 provides preliminary guidance regarding methods that the NRC staff may find acceptable if an SMR or non-LWR applicant or licensee would elect to implement the alternative physical security requirements in the proposed limited-scope rule.

3.1 Proposed alternative requirement for armed responders

The first proposed alternative physical security requirement would permit an eligible SMR or non-LWR applicant or licensee to be relieved from the current requirement for a minimum number of armed responders. Under the limited-scope rule, the SMR or non-LWR applicant or licensee would be permitted to design a physical protection program that could potentially have fewer than 10 onsite armed responders, if appropriate. SMR and non-LWR applicants and licensees would use existing methods, such as those used by operating reactor licensees, for determining the necessary number of onsite armed responders.

For an eligible SMR or non-LWR applicant or licensee that designs its physical protection system to rely on onsite armed responders to interdict and neutralize the DBT, the proposed physical security alternative would provide relief only from the prescriptive requirement for the minimum number of armed responders; all other existing requirements associated with onsite armed personnel would continue to apply. The SMR or non-LWR applicant or licensee would be able to reduce the number of onsite armed responders to zero if the applicant or licensee would also implement the proposed alternative measure that would allow it to rely on law enforcement or other offsite armed responders to interdict and neutralize the DBT (see section 3.2 below).

3.2 Proposed alternative requirements for interdiction and neutralization

The second proposed alternative security requirement would allow an eligible SMR or non-LWR applicant or licensee to rely on law enforcement or other offsite responders (e.g., proprietary or contract security personnel controlled by a licensee), rather than onsite armed responders, to interdict and neutralize the DBT adversary. The proposed rule would not create any NRC regulatory jurisdiction over, or requirements for, law enforcement responders. The proposed alternative security requirement would also not relieve an eligible SMR or non-LWR applicant or licensee from the existing responsibility to interdict and neutralize threats up to and including the DBT of radiological sabotage; rather, it would provide an applicant or licensee with an alternative method for fulfilling these responsibilities. Applicants and licensees implementing this requirement would be required to:

(1) Provide adequate delay to enable law enforcement or other offsite armed responders to interdict and neutralize threats up to and including the DBT,
(2) Provide necessary information about a facility to law enforcement or other offsite responders,
(3) Document law enforcement or other offsite responders' role(s) in site's safeguards contingency plans,
(4) Provide periodic training to those responders to support site-specific preparedness to fulfil the interdiction and neutralization functions in safeguards contingency events at licensee sites (i.e., within the owner-controlled area, the protected area(s), vital areas, and other site facilities), and
(5) Identify criteria and measures to compensate for the degradation or absence of law enforcement or other offsite armed responders and propose suitable compensatory measures that meet the requirements in the regulations to address this degradation.

Unlike onsite armed responders, which are required by existing regulations to be available at the site for response, an eligible SMR or non-LWR applicant or licensee that would rely upon law enforcement or other offsite armed responders would be required to consider the possibility that offsite response may be impeded by events outside, or independent from, a safeguards event at the site. For example, a law enforcement department relied upon for response may decide to disband its tactical response team or discontinue its support to a licensee. Because the existing requirement in the regulations is specific to security systems and equipment performing required functions, the addition of the proposed alternative requirement for interdiction and neutralization would create the potential for degradation or unavailability of the personnel relied on to perform security functions, such as interdiction and neutralization. As such, the proposed requirement would expand the requirements in the regulations for establishing suitable compensatory measures to address the degradation or loss of interdiction and neutralization functions.

Applicants and licensees relying on offsite responders other than law enforcement would be required to meet all existing security response, training, and qualification requirements, except for some location-related requirements in the regulations. Eligible SMR and non-LWR applicants and licensees relying on law enforcement responders for interdiction and neutralization of the DBT adversary would be exempt from several response requirements in the regulations and most of the security training and qualification requirements in the regulations because those requirements would be performed by the relevant law enforcement organization(s). One set of requirements from which an applicant or licensee would not be relieved would be the performance evaluation program requirements related to armed response personnel. An applicant or licensee would be required to satisfy the performance evaluation program requirements for all armed response personnel, including law enforcement, because a performance evaluation program would provide assurance that a licensee that relies on law enforcement or other offsite armed responders for the contingency response and interdiction and neutralization functions can protect a site against the DBT. The implementation of a performance evaluation program would provide assurance that any vulnerabilities or weaknesses resulting from the reliance on law enforcement or other offsite responses to safeguards contingencies would be identified and corrected and that a licensee would maintain an adequate response.

3.3 Proposed alternative requirements for physical barriers

The third proposed alternative physical security requirement would permit eligible SMR or non-LWR applicants or licensees to use means other than physical barriers in the design of their physical protection systems. Applicants and licensees would be permitted to consider other methods that include the use of reliable and available engineered systems or human actions to provide the delay that would be necessary to facilitate security responses after the successful detection and assessment of threats up to and including the DBT. For example, applicants and licensees would be able to:

(1) Use engineered systems designed to disperse material that physically impedes or physiologically interferes with the adversary, such as obscurants (e.g., cold smoke), irritants (e.g., active denial systems), and stick foams, rather than physical barriers, to provide delay;
(2) Consider the delay provided by active engineered security systems used for interdicting and neutralizing the adversary (e.g., remotely operated weapons systems), which can increase adversary task or travel times, interrupt adversary action, or serve other delay functions (e.g., channelling);
(3) Rely on physical spatial distances, terrain, and other natural features that, after successful detection and assessment, would provide delay by increasing adversary task times; and
(4) Consider methods other than physical barriers as physical access controls when implementing their access authorization programs, including restricting access to vital areas.

3.4 Proposed alternative requirements for onsite secondary alarm stations

The fourth proposed alternative physical security requirement would permit eligible SMR and non-LWR applicants and licensees to locate a secondary alarm station offsite, provided that its capabilities would continue to be redundant and equivalent to an onsite central alarm station. Implementation of this alternative could include, for example, having a co-located alarm station offsite that provides secondary alarm station functions for multiple reactor sites or using a certified commercial security service.

Eligible SMR or non-LWR applicants or licensees electing to use an offsite secondary alarm station would be relieved from meeting several existing security requirements. For example, they would be relieved from the requirements to construct, locate, and protect the secondary alarm station to the same standards as the central alarm station. Applicants and licensees would also not need to locate an offsite secondary alarm station inside a protected area, ensure that the interior of the secondary alarm station is not visible from the perimeter of the protected area, or construct the secondary alarm station to be bullet resistant. Applicants and licensees would be permitted to install equipment in offsite secondary alarm stations that is different than the equipment in their central alarm stations, as long as the secondary alarm stations can perform the equivalent and redundant functions of the central alarm stations. Finally, they would not be required to designate offsite secondary alarm stations as vital areas or locate the secondary power supply systems for offsite secondary alarm stations in vital areas.

4. PROPOSED ALTERNATIVE REGULATORY FRAMEWORK—THE 10 CFR PART 53 RULE

In order to comply with NEIMA, the NRC staff proposed an alternative regulatory framework for licensing and regulating future commercial nuclear power plants. This alternative framework, to be added to the NRC's regulations under a new 10 CFR Part 53, would adopt technology-inclusive approaches and use risk-informed and performance-based techniques to ensure an equivalent level of safety to that of operating commercial nuclear plants, while providing flexibility for licensing and regulating a variety of technologies and designs for commercial nuclear reactors. Unlike the proposed limited-scope rule, the proposed Part 53 would apply to all new reactor designs and sizes, rather than only SMRs and non-LWRs, and would provide new reactor applicants and licensees with maximum flexibility with which to design their physical protection programs.

One unique provision of the proposed 10 CFR Part 53 framework would be a graded approach to establish physical protection program requirements for new reactor applicants and licensees. There would be two physical protection-related paths to consider:

(1) The first path would be to establish, implement, and maintain a physical protection program that would adequately defend against the DBT of radiological sabotage by satisfying the requirements in either a proposed new regulation (10 CFR 73.100) or the existing power reactor security rule, including any of the four alternative physical security requirements that would be implemented if the NRC finalizes the proposed limited-scope rule.
(2) The second path would be to demonstrate that protecting against the DBT is unnecessary to protect public health and safety and the environment, such that a lesser level of security is appropriate. To avoid having to defend against the DBT under the proposed 10 CFR Part 53 framework, a new reactor applicant or licensee would need to demonstrate that the radiological consequences from a DBT-initiated attack would result in offsite doses below the values in the proposed 10 CFR Part 53, even if licensee mitigation and recovery actions, including any operator action, are unavailable or ineffective.

It is important to note that although both the proposed 10 CFR Part 53 rule and the proposed limited-scope rule would include requirements for performing an analysis of the offsite radiological consequences resulting from a postulated DBT attack, there would be important differences between those two analyses. First, an applicant or licensee performing the consequence analysis required by the proposed limited-scope rule would be able to consider a limited number of security features that could mitigate the capabilities of an DBT adversary. Second, the relief that an applicant or licensee could obtain under the proposed limited-scope rule would be limited to implementing the four proposed alternative requirements. Allowing consideration of some security features would be appropriate because risk would be addressed primarily by controlling application (i.e., only SMR and non-LWR designs) and requiring applicants and licensees to continue to defend against the DBT. Under the proposed 10 CFR Part 53 framework, new reactor applicants and licensees would have to assess the potential offsite radiological consequences of a postulated, unmitigated DBT attack. If they were to demonstrate that consequences would be below reference dose values, new reactor applicants and licensees would be exempt from having to defend against the DBT and would not be subject to NRC force-on-force inspections; instead, they would be permitted to establish, implement, and maintain physical protection programs similar to those to protect special nuclear material of moderate and low strategic significance or Category 1 or 2 radioactive material, as applicable.

Another major provision of the proposed 10 CFR Part 53 rule would be the creation of a performance-based physical security regulatory framework under section 10 CFR 73.100. Unlike the combination of performance criteria and prescriptive requirements used by the existing security framework for nuclear power reactors, the proposed security requirements in 10 CFR 73.100 would primarily rely on performance objectives and requirements, giving new reactor applicants and licensees maximum flexibility for determining how to demonstrate adequate protection against the DBT. New reactor applicants and licensees would be required to provide defense in depth through the integration of engineered systems, administrative controls, and management measures, and through the diversity, independence, separation, and redundancy of physical security systems to ensure their reliability and availability.

Some examples of the physical protection system design requirements that would be established under the proposed 10 CFR 73.100 are outlined below. The proposed 10 CFR 73.100 would contain additional performance standards for other security system design requirements that are not discussed in this paper, including access control; personnel and vehicle searches; insider threat mitigation; training, qualification, and performance testing of security personnel; cybersecurity; and security equipment maintenance and testing. On February 2, 2024, the NRC released preliminary Draft Regulatory Guide DG-5076, "Guidance for Technology-Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants." DG-5076 provides preliminary guidance regarding methods that the NRC staff may find acceptable if a new reactor applicant or licensee would elect to implement the alternative physical security framework in the proposed 10 CFR 73.100.

4.1 Proposed intrusion detection and assessment requirements

New reactor applicants and licensees would be required to be capable of detecting attempted and actual unauthorized access to interior and exterior areas containing structures, systems, and components needed to

implement safety and security functions. They would also be required to be capable of timely assessment for determining the cause of a detected intrusion.

4.2 Proposed security communications requirements

New reactor applicants and licensees would be required to maintain continuous security communications even when subjected to the DBT adversary's ability to disable or disrupt communications.

4.3 Proposed security response requirements

4.3.1 New reactor applicants and licensees' physical protection programs would be required to be designed to provide timely security response to interdict and neutralize threats up to and including the DBT. Their programs would also be required to have layers of security response, with each layer assuring that a single failure would not result in the loss of capability to neutralize the DBT adversary.

4.3.2 Structures, systems, and components relied on for delay would be required to be designed to facilitate interdiction and neutralization of the DBT adversary. Physical barriers used for delay would not be required to be configured in accordance with existing prescriptive requirements, which would enable new reactor applicants and licensees to employ, for example, fences that would no longer need to be configured in accordance with the regulations.

4.3.3 New reactor applicants and licensees would be permitted to rely on law enforcement or other offsite responders to interdict and neutralize the DBT adversary if they implement and follow the same requirements as those contained in the proposed limited-scope rule.

4.4 Proposed requirements for protecting against land and waterborne vehicle borne bomb assaults

New reactor applicants and licensees would be required to be capable of protecting a plant against the DBT vehicle bomb assault by ensuring that any methods they use for that purpose will protect the reactor building(s) and structures containing safety or security-related structures, systems, and components from explosive effects.

4.5 Comparing the NRC's two proposed physical security regulatory frameworks

Figure 1 summarizes a few of the basic differences between the two proposed security regulatory frameworks that the NRC is currently considering.

Rulemaking Purpose	Physical Security for Advanced reactors (Limited Scope Rule)	Physical Security for Part 53
Increased flexibility for physical security	Yes, via the specific alternatives to 73.55 prescriptive requirements	Yes, through new performance-based requirements in 73.100. Option to implement traditional 73.55 requirements and alternatives
Potential relief from requirement to protect the site against the Design Basis Threat (DBT) of radiological sabotage	No (only through exemption request)	Yes, if a licensee can demonstrate that potential consequences resulting from a DBT attack would not lead to offsite radiation hazards that would endanger public health and safety
Cyber security	No changes	Option of using the 10 CFR 73.110 graded approach or the legacy 10 CFR 73.54 framework
Access Authorization	No changes	Graded approach based on consequence
Fitness for Duty	No changes	Graded approach based on consequence

FIG. 1. Rulemaking options for the limited-scope rule and Part 53 rulemaking.

5. CONCLUSION

All three NRC security regulatory frameworks discussed in this paper are designed to ensure that commercial nuclear power reactor licensees' physical protection programs and systems can adequately defend against the NRC's DBT of radiological sabotage, when necessary. For over 40 years, the NRC and its operating power reactor licensees have been relying on compliance with the physical security requirements in the existing 10 CFR 73.55 to provide reasonable assurance of adequate protection. A proposed limited-scope rule that would add a subsection to that existing security regulatory framework would consider the reduced risk that may be posed by certain new reactor designs and minimize the need some new reactor applicants and licensees to obtain exemptions or alternative measures on a case-by-case basis. The alternative physical security requirements in the proposed subsection(s) would also provide greater flexibility to a subset of eligible new reactor applicants and licensees as they design their physical protection programs. Should any new reactor applicants or licensees want to use different methods for providing fundamental security functions from those prescribed by the existing or proposed regulations, or be able to demonstrate that their reactor facility designs would result in offsite radiological consequences from an unmitigated DBT attack that would be below the required dose reference values, the security framework in the proposed 10 CFR Part 53 rule would enable new reactor applicants or licensees to implement and maintain physical security protection programs commensurate with a facility's risk.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Lou Cubellis, Amanda Marshall, and Francis Paul Peduzzi of the NRC staff for their invaluable contributions and support throughout the development of this paper. Their guidance, assistance, and leadership have been instrumental in the shaping of this work.

REFERENCES

[1] Code of Federal Regulations, Title 10, "Energy," Part 50, "Domestic Licensing of Production and Utilization Facilities."

[2] Code of Federal Regulations, Title 10, "Energy," Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

[3] Code of Federal Regulations, Title 10, "Energy," Part 73, "Physical Protection of Plants and Materials."

[4] Federal Register, Volume 73, page 60612, October 14, 2008.

[5] Public Law No. 115-439, "Nuclear Energy Innovation and Modernization Act," January 14, 2019.

[6] U.S. NRC, Staff Requirements Memorandum (SRM) on SECY-16-0073, "Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088," October 5, 2016.

[7] U.S. NRC, Staff Requirements Memorandum on SECY-18-0076, "Options and Recommendations for Physical Security for Advanced Reactors," November 19, 2018.

[8] U.S. NRC, Preliminary Draft Regulatory Guide DG-5072, "Guidance for Alternative Physical Security Requirements for Small Modular Reactors and Non-Light Water Reactors" (Agencywide Documents Access and Management System (ADAMS) number ML23263A997), February 2, 2024.

[9] U.S. NRC, Preliminary Draft Regulatory Guide, DG-5076, "Guidance for Technology-Inclusive Requirements for Physical Protection of Licensed Activities at Commercial Nuclear Plants" (ADAMS number ML23286A282), February 2, 2024.