NUCLEAR ENERGY INSTITUTE

WHITE PAPER

PROPOSED CONSEQUENCE-BASED PHYSICAL SECURITY FRAMEWORK FOR SMALL MODULAR REACTORS AND OTHER NEW TECHNOLOGIES

November 2015

ACKNOWLEDGMENT
This NEI White Paper was developed by the NEI Small Modular Reactor Working Group.

WHITE PAPER

PROPOSED CONSEQUENCE-BASED PHYSICAL SECURITY FRAMEWORK FOR SMALL MODULAR REACTORS AND OTHER NEW TECHNOLOGIES

I. Introduction

The purpose of this paper is to discuss generic policy and technical issues associated with security for small modular reactors (SMRs) and other new technologies, such as non-light-water reactors (non-LWRs), that have not been addressed to-date, and to propose a consequence-based physical security framework that is more appropriate for these designs. . The Nuclear Energy Institute would like to work with the NRC staff to address these policy and technical issues and develop a consequence-based regulatory framework for physical security. To this end, this paper is intended to provide a basis for further discussion of next steps toward providing clarity concerning security requirements for SMRs and other new technologies.

A consequence-based security framework is needed for SMRs and other new technologies, because the existing regulatory framework does not contemplate the significant reduction in risks that these designs achieve through enhanced safety and security features. Furthermore, a consequence-based approach is needed to avoid imposing undue regulatory burden on these designs, and to incentivize designers to reduce reliance on human actions by enhancing security through engineered features. Timely NRC consideration and feedback on the acceptability of a consequence-based security framework for SMRs and other new technologies, and the associated policy and technical issues, is needed to inform design and business decisions affecting certification, licensing and deployment of SMRs over the next several years. As discussed below, consideration of such an approach would be consistent with the NRC's Advanced Reactor Policy Statement.

The framework discussed in this paper is rooted in the objective of physical security to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material.[1] The framework would continue to require facilities to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety. Designs that meet this requirement based upon the performance of engineered features and without reliance on interdiction or neutralization of the design basis threat by the site's security response force (referred to as "provide security by design") would be required to detect, assess, and communicate any unauthorized penetration (or such attempts) to off-site responders (i.e., local law enforcement). This approach would incentivize the use of engineered features to enhance the security posture, assure that the facility's security response capabilities are commensurate with the risk of off-site dose consequences, and would address other policy and technical issues related to physical security for SMRs and other new technologies.

---

[1] The discussion in this paper is mainly focused on the requirements related to protect against acts of radiological sabotage, as it is envisioned that SMRs and other new technologies will prevent theft and diversion of special nuclear material similar to the currently operating reactors.

This framework would be applicable to SMRs and other new technologies, which are capable of protecting against acts of radiological sabotage through engineered features, and reducing, or eliminating, reliance on human actions. Such a framework is appropriate for these facilities because the enhanced safety and security features being designed into SMRs and other new technologies can significantly reduce the risk of theft, diversion and radiological sabotage associated with the design basis threat. The proposed framework can be established generically, without site or design specific information regarding source term, target sets, physical barriers or projected off-site doses. Existing nuclear power plants in operation or under construction would continue to meet the existing requirements, which are based on the potential consequences for those designs. For such reactors, the existing requirements provide adequate protection of the public health and safety from the design basis threat and it would neither result in a substantial increase in the overall protection of public health and safety, nor be cost-effective for these facilities to modify engineered plant systems or physical barriers.

The concepts in this paper are consistent with the concepts that form the basis for the NRC's decision, in SRM-SECY-15-0077, to approve the staff's recommendation to initiate a rulemaking to revise regulations and guidance for emergency preparedness (EP) for SMRs and other new technologies. The staff's recommendation in SECY 15-0077 was based on the conclusion that "SMRs could [sic] have reduced off-site dose consequences in the unlikely event of an accident, although this has not yet been verified" and the goal to "establish EP requirements for SMRs and other new technologies that are commensurate with the potential consequences to public health and safety, and the common defense and security at these facilities." As Chairman Burns noted in his vote sheet on SECY-15-0077, such an approach (to pursue a generic framework through rulemaking, rather than apply existing requirements and process exemption requests) "will provide greater regulatory stability and more opportunity for external stakeholder involvement in the development of EP requirements for SMRs and other new technologies." There are numerous parallels between the basis for an EP framework appropriate to SMRs and other new technologies, and a security framework appropriate to these same designs. Most notably are the reduction of risk of off-site dose consequences and the undue burden that existing requirements would impose on these designs. Thus, the basis for and expected benefits of a consequence-based approach to physical security requirements for SMRs and other new technologies, discussed in this paper, are similar to those as the basis for the ongoing rulemaking for EP for these same designs.

II. Background on NRC Security Requirements

NRC security requirements are set forth in 10 CFR Part 73, "Physical Protection of Plants and Materials," and are incorporated by reference for nuclear power reactors under the licensing regulations of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." These security requirements are focused on protecting against acts of radiological sabotage and preventing theft or diversion of special nuclear material. 10 CFR 73.55 contains performance-based and prescriptive security requirements that require nuclear power plants to establish and maintain a physical protection program that protects against the design basis threat and prevents significant core damage and spent fuel sabotage as the means to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

NRC regulations define the design basis threat based upon adversary characteristics, which are independent of the design features of the facility or the technology of the nuclear power plant. The NRC requires nuclear power plants to have physical barriers, to identify target sets, and to have a security organization with the capabilities to detect, assess, interdict and neutralize the design basis threat. Target sets are defined as a minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core disruption) or spent fuel sabotage (e.g., draining the spent fuel pool leaving the spent fuel uncovered for a period of time, along with the fuel heat up and the associated potential for release of fission products) barring extraordinary actions by plant operators.[2] In this manner, the size of the security organization consists of a sufficient number of armed responders (a minimum of ten armed security responders is required per 10 CFR 73.55(k)(5)(ii)) capable of interdicting and neutralizing the design basis threat in order to protect the target sets.

NRC requires nuclear power plants to have a Physical Security Plan, a training and qualification plan, security contingency plans, access authorization program, insider mitigation program, and a cyber security plan. Nuclear plants are required to demonstrate the effectiveness of the security organization through force-on-force activities, coordinate with other onsite plans and procedures, and provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures.

The regulation in 10 CFR 73.55(r) allows applicants to propose alternative methods or approaches to meet the security requirements that offer equivalent protection and meet the same high-assurance performance objectives for requirements specified in 10 CFR 73.55(b). Applicants may also request exemptions to address specific unique characteristics of the design and operation of a particular technology. However, these processes are not efficient or preferred to address generic policy or technical issues that may apply more broadly to a class of technology. In fact, when generic policy and technical issues exist, it is important (and efficient) for the agency to address these issues through rulemaking and guidance.

SECY 10-0034, *Potential Policy, Licensing, and Key Technical Issues for Small Modular Nuclear Reactor Designs*, identified security and safeguards requirements as potential policy issues for integral pressurized-water reactor (iPWRs) and non-LWRs, and discussed the NRC's plans to resolve these issues. In SECY 11-0184, *Security Regulatory Framework for Certifying, Approving, and Licensing Small Modular Nuclear Reactors*, the NRC staff concluded that "the current security regulatory framework is adequate to certify, approve, and license iPWRs" and non-LWRs. This conclusion was based in part on the NRC's determination that "provisions for alternative measures, license conditions and exemptions provide flexibility for applicants to achieve the objective of high assurance that activities are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety." NEI issued a Position Paper titled, *Physical Security for Small Modular Reactors* on July 31, 2012 that

[2] NRC SECY-08-0099, "Final Rulemaking – Power Reactor Security Requirements (RIN 3150-AG63)"

identified several unique considerations for physical security for SMRs based on iPWR technology that may cause the need for reactor vendors to seek exemptions to certain regulations. While industry concedes that SMRs and other new technologies could comply with the current regulatory framework for physical security, we do not believe that doing so is appropriate for these designs. On the contrary, 10 CFR Part 73 requirements promulgated to apply to large LWRs appear to be overly rigid and burdensome for these designs, as discussed below.

Subsequent to these earlier papers, the nuclear industry determined that a consequence-based physical security framework, which is technology-neutral, dose-based, and risk-informed would be more appropriate and could be effectively implemented for SMRs and other new technologies. The goal of the consequence-based regulatory framework for physical security is to protect against acts of radiological sabotage and prevent theft or diversion of special nuclear material in a more effective and efficient manner.

III. Engineered Features of Small Modular Reactors and Other New Technologies

A nuclear power plant's engineered features consist of systems, structures and components (SSCs) that provide safety, and physical barriers that provide security. Together, these engineered features are used in the identification of target sets and in the protection of the target sets from the design basis threat.

SMRs and other new technologies will be designed to address the Commission's policy statement on the regulation of advanced reactors (73 Federal Register (FR) 60612, October 14, 2008), which states in part that "the Commission expects, as a minimum, at least the same degree of protection of the environment and public health and safety and the common defense and security that is required for current generation light-water reactors (LWRs) [licensed before 1997]" and that "the Commission expects that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions."

SMRs and other new technologies have the opportunity to augment the site's engineered features in order to provide enhanced safety and security, in a manner that reduces the reliance on human actions. The degree to which a particular design protects against radiological sabotage by design depends on whether the addition of engineered features, beyond those necessary to comply with the regulations, is cost effective. Such an approach, which would increase the capital costs of the plants, may be advantageous if there is an opportunity to reduce operating costs through right-sizing the security staff in a manner appropriate with the potential off-site consequences. For applicants that pursue this approach, they will need to demonstrate the effectiveness of the engineered features of their designs in protecting against radiological sabotage.

Enhanced Safety Features

The LWR SMR designs currently in development and the advanced reactor design concepts currently being discussed have grown out of a desire to provide enhanced levels of safety while at the same time providing reliable, cost-competitive electricity and other energy products. Many of these designs incorporate fewer, simpler and passive SSCs that reduce reliance on operator actions, electrical power and additional sources of coolant in order to perform their safety functions. Often, these enhanced safety features contribute to enhance protection against acts of radiological sabotage by increasing the minimum combination of equipment or operator actions that are included in the target set, and/or eliminating target sets altogether.

These designs significantly reduce the risk of radiological release and off-site dose consequences because they have smaller cores and source terms, simplified designs that reduce potential accident sequences, and slower accident progressions that permit more time for mitigation. The following provides additional details about the enhanced safety features for some LWR SMRs, and their potential to protect against security based events:[3]

Smaller Core Fission Product Inventories – The NRC defines SMRs as the class of reactors with a licensed thermal power rating ≤1,000 MWt (≤300 MWe), which translates to smaller core sizes and less thermal output. Current SMR designs have cores that are physically smaller in both the radial and vertical directions and contain fewer fuel assemblies as compared to traditional reactors. Accordingly, the amount of radiological material available for potential release is greatly reduced. This results in smaller source terms and lower decay heat levels following a reactor shutdown, and leads to a corresponding reduction in risk of off-site dose consequences regardless of the initiating event.

Improved Design Features – The following are some of the more common safety enhancements incorporated into the LWR SMR designs, although not all of these features are applicable to all designs. Notably many of these enhanced safety features reduce the risk of off-site dose consequences regardless of initiating event.

- An integral reactor vessel design eliminates large-break Loss-of-Coolant Accidents (LOCA) by eliminating large-bore piping in the design and reactor vessel penetrations below the top of the core.

- Fuel and reactor components are largely or completely located below ground level, resulting in the reduction or elimination in postulated release paths and impacts of external hazards (e.g., tornado missiles, aircraft impacts), and improved protection against external adversarial assaults (e.g., vehicle bomb attacks).

- A large water volume relative to the thermal power is available for cooling and shielding. The larger volume-to-break-size ratios also result in slower accident progression assumptions. The volume of water is sufficient such that fuel failure is not postulated to occur for many hours or days following the onset of an accident condition.

- The postulated short-term (accident) release path goes through pools surrounding the containment, reducing the risk of off-site dose consequences due to an event that causes significant core damage.

---

[3] It is anticipated that advanced non-LWR reactors will also incorporate these, and other, safety enhancements, as applicable to the specific technology of the design. However, due to the limited information available on non-LWR technologies at this time, it is not practical to describe their potential safety features.

- A greater number of reactor coolant pumps results in a smaller impact from loss of a single pump, increasing the number of pumps that are included in the target set.

- Use of natural circulation for the primary loop during both normal operations (e.g., full power, shutdown) and post-accident conditions results in lower core flow rates, lower core heat flux, larger margins to departure from nucleate boiling (DNB), lower peak cladding temperatures, and reductions in stored energy and fuel centerline temperatures.

Slower Accident Progression – LWR SMR design features, such as those described above, result in a lower likelihood of fuel damage, a longer time to any fuel failure, and significant reduction in accident consequences. In addition, the ability to mitigate or accommodate long-term consequences of significant core damage or spent fuel sabotage is enhanced, as power and water demands to maintain the plant in a safe condition are greatly reduced, easily accommodated, or eliminated altogether.

Enhanced Physical Barriers

SMRs and other new technologies have the opportunity to enhance the nuclear power plant's physical security barriers early in the design process in a manner that considers a balanced approach to security, operations and cost objectives. These physical barriers can enhance the security posture through design by protecting the target sets from the design basis threat, up to and including preventing the design basis threat from damaging the target sets in a manner that would cause off-site dose consequences that constitutes an unreasonable risk to the public health and safety. Conceptually, the types of physical barriers that would be incorporated into these designs are similar to those used in existing nuclear power plants, although they could also be based upon new and innovative technologies. The following provides additional details about the enhanced physical barriers that SMRs and other new technologies may incorporate:

- Optimize the multiple (redundant) layers of fixed (passive) barriers to the safety-related equipment included in target sets to prevent access by the design basis threat.

- Optimize the location, size, shape, and orientation of structures, buildings and physical barriers to increase the time and resources the design basis threat would expend in order to gain access to safety-related components included in target sets.

- Further minimize access points to the facility in general and to the safety-related equipment included in target sets contained within the protected area.

- Locate and configure safety-related components such that even if the design basis threat gains access to these items, it would not be possible for the design basis threat to damage these items in a manner that would cause off-site dose consequences that constitute an unreasonable risk to the public health and safety.

- Incorporate new or enhanced technologies for automatic detection, assessment, delay and communication systems.

IV. Proposed Consequence-Based Regulatory Framework for Physical Security

The existing NRC security regulations were developed based upon the characteristics of large LWRs comprising the U.S. fleet of nuclear power reactors. As nuclear reactor designs evolve to incorporate advanced safety and security features, it is important that the regulatory framework also evolve in a manner that reflects these features and allows for more efficient means to protect public health and safety. It is reasonable to establish a consequence-based security framework for SMRs and other new technologies because advances in these designs are expected to reduce the reliance on security response capabilities to protect against acts of radiological sabotage.

The objective of the consequence-based security framework is to meet the existing general requirement to "provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." However, inherent in the existing requirements is the presumption that, absent a response from the security organization that "interdicts and neutralizes" the design basis threat, the design basis threat is capable of causing significant core damage and spent fuel sabotage, and that these outcomes would result in off-site radiological consequences that present an unreasonable risk to public health and safety. Thus, the regulations, as currently written, do not contemplate designs for which one of the following can be achieved:

1. Engineered features alone prevent the design basis threat from causing significant core damage or spent fuel sabotage, without reliance on the interdiction or neutralization of the design basis threat by the site's security response force.
2. Off-site radiological consequences do not constitute an unreasonable risk to the public health and safety, even in cases where the design basis threat is capable of causing significant core damage or spent fuel sabotage.

It is feasible, and indeed likely, that SMRs and other new technologies that incorporate enhanced safety and security features will achieve one of the aforementioned consequence-based standards not currently contemplated by the regulations. Thus, a consequence-based regulatory framework is needed to establish appropriate requirements for SMRs and other new technologies. Clearly, each individual design would need to demonstrate to the satisfaction of the NRC its ability to achieve the performance criteria associated with a consequence-based security framework.

A consequence-based regulatory framework for SMRs and other new technologies would ensure that the role of the security organization, including the response capabilities, is commensurate with the risks for designs that can provide physical security by-design. For these facilities, there would be no need for the security organization to "interdict and neutralize" the design basis threat, as the engineered features of the nuclear plant provide security equal to or in excess of the design basis threat's capabilities, such that the design basis threat is not capable of causing off-site dose consequences that constitute an unreasonable risk to the public health and safety. Instead, the consequence-based regulatory framework analog to the requirements in 10 CFR 73.55(b)(3)(i), 10 CFR 73.55(k)(1), and 10 CFR 73.55(k)(8)(ii) for power reactors would only require the response of the security organization to "detect, assess, and communicate any unauthorized penetration (or such attempts) to a designated off-site response force (i.e., local law enforcement)." Satisfaction of this requirement provides high assurance that activities involving special nuclear material are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety, because the engineered features protect against acts of radiological sabotage, and local law enforcement interdicts the adversaries. Accordingly, there is no need to specify requirements for armed responders, and the consequence-based security framework would not contain the requirements for armed responders currently found in 10 CFR 73.55(b)(6), 10 CFR 73.55(k)(4), 10 CFR 73.55(k)(5), and 10 CFR 73.55(k)(5)(ii) for power reactors.

A consequence-based framework would not remove altogether the need for a security organization. Indeed a security organization would still be required to perform the functions of "detect, assess and communicate" as well as other functions delegated to the security organization, including access authorization, vehicle searches, development and maintenance of security plans, and providing escorts. Licensees would also develop and maintain a Documented Integrated Response Plan for coordinating local law enforcement response. This framework would also not prohibit the capability of security officers from being armed, although the nature of the armaments could vary based upon the role of the security organization.

The concept of security requirements commensurate with the off-site radiological risk, including an increase reliance on the engineered features and a decreased reliance on the security organization's response, is not new. 10 CFR 73.25, "Performance capabilities for physical protection of strategic special nuclear material in transit," 10 CFR 73.45, "Performance capabilities for fixed site physical protections systems," and 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste" credit the engineered features of the designs and require the security response organization to "detect, assess and communicate," commensurate with the risks these design pose to public health and safety. SMRs and other new technologies may also protect against acts of radiological sabotage, based upon the engineered features, without reliance on a security response force to interdict or neutralize the design basis threat, and thus a consequence-based regulatory framework should be established for these technologies.

Additional Policy and Technical Issues

In addition to the potential changes to security organization requirements, the NRC should assess whether additional changes to security requirements, policy and guidance may be needed to implement a consequence-based regulatory framework based upon the enhanced safety and security features of SMRs and other new technologies.

The following are examples of some additional policy and technical issues that need to be addressed for SMRs and other new technologies:

1. Appropriate dose-based criteria are needed to assess a licensee's performance to protect against "radiological sabotage." The current NRC criterion is to "prevent significant core damage and spent fuel sabotage" as the means to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. For SMRs and other new technologies these are not the most appropriate performance criteria. Instead the performance criteria should be based upon the risk of off-site radiological

consequences from the design basis threat. One option could be to replace the definitions of significant core damage and spent fuel sabotage (currently defined as non-incipient, non-localized fuel melting and/or core disruption; and draining the spent fuel pool leaving the spent fuel uncovered for a period of time, along with fuel heat up and the associated potential for release of fission products, respectively) with definitions based upon acceptance limits for off-site doses. Another option could be to replace the performance criteria for SMRs and other new technologies to "prevent significant core damage and spent fuel sabotage" altogether with a dose-based acceptance criteria. Consideration of this issue may also need to reflect upon prior Commission decisions related to the applicability of radiological dose criteria to physical security requirements. In doing so, it should be recognized that there are significant differences between the characteristics of SMRs and other new technologies, and the characteristics of existing large LWRs that were important in forming the underlying basis of the Commission's prior decisions. Thus, it is reasonable to expect that the bases for the NRC's prior decision to establish performance criteria based upon "significant core damage and spent fuel sabotage" are not applicable to SMRs and other new technologies, and that the characteristics of these new designs could support a regulatory basis for dose-based performance criteria.

2. The role of probabilistic risk assessment (PRA) and establishment of PRA acceptance criteria should be evaluated when defining a dose-based performance criteria that demonstrates that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The use of PRA in the area of physical security is not new, and is currently being used in the identification of target sets. However, it may be appropriate for the role of PRA to be expanded for a consequence-based security framework. For example, probabilistic methods could be used to determine a more risk-informed assessment of off-site dose-consequences resulting from security threat based event scenarios, with associated PRA acceptance criteria that are consistent with the NRC's Safety Goal Policy and Quantitative Health Objectives.

3. Requirements should be established for facilities for which the engineered features alone result in extremely low off-site radiological risks, but which rely upon a limited and focused security response (e.g., in terms of the number of responders, number of locations to protect, and duration of the response) in order to protect against radiological sabotage. These facilities may be able to meet the performance criteria with security response capabilities that are less than those currently required by the existing regulations (e.g., reliance on less than the currently requirement minimum of 10 armed responders, and without the need to interdict or neutralize). Thus, requirements for these facilities should ensure that the security response capabilities are commensurate with the risks. For example, these facilities may be required to have security response capabilities that are greater than would be required in the proposed approach, but less than those required by the existing regulations. These facilities may be required to delay the design basis threat until local law enforcement can interdict, in addition to the requirements to detect, assess, and communicate any unauthorized penetration (or such attempts) to off-site responders (i.e., local law enforcement).

4. The applicability of requirements in 10 CFR 73.55(k) for response, including the requirements for maintaining firearms and ammunition in working order and available for use, training and qualification, and the use of deadly force, should be assessed for a consequence-based security framework.

5. The applicability of requirements and guidance for force-on-force (FOF) exercises (e.g., 10 CFR 73.46(b)(9) and Appendix B to 10 CFR Part 73), should be assessed for a consequence-based security framework.

6. Development of more realistic assumptions on the effectiveness of physical barriers, based upon research and testing that confirm their performance and produce data that can be used to validate computer codes, should be assessed for a consequence-based security framework.

7. Prevention of theft or diversion of special nuclear material would need to be addressed, including the potential for alternative bases for innovative fuel designs.

V. Advantages of a Consequence-Based Security Framework

A consequence-based physical security framework for SMRs and other new technologies can provide a more effective and efficient approach to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. Security is a key factor in the business case for the feasibility and development for SMRs and other new technologies, because compliance with the security requirements is a large component of the facility's operating and maintenance costs. Establishing such a framework would offer a number of additional benefits including:

1) Promotion of regulatory stability, predictability, and clarity in the licensing process of SMRs and other new technologies for the NRC staff and potential vendors and applicants;
2) Recognition of, and appropriate credit for, security enhancements of SMRs and other new technologies, including those embedded in passive and enhanced safety features;
3) Incentives for security by-design and reduced reliance on human actions; and
4) Opportunity for public engagement on the issues related to security for SMRs and other new technologies.

The establishment of a consequence-based physical security framework would appropriately credit the ability of engineered design features to protect against acts of radiological sabotage, and appropriately define the requirements for the security organization. This approach is needed to avoid imposing undue regulatory burden on facilities that provide physical security by-design, and permit these designs to protect the public health and safety more effectively and efficiently. It would also incentivize the use of cost-effective innovative design features and enhanced physical barriers in the design of these technologies, with reduced reliance on human actions. This is consistent with the NRC's Advanced Reactor Policy Statement, which encourages new reactor designs to "…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."

VI. Recommendation

We recommend a public meeting in early 2016 to get the staff's feedback and discuss next steps toward providing clarity concerning security requirements for SMRs and other new technologies, including feedback on the acceptability of a consequence-based approach, development of technical basis and guidance, and the need for rulemaking and Commission engagement, as appropriate. Establishing a consequence-based security framework now, rather than waiting to address these generic policy and technical issues through the review of each specific application, would enable designs to incorporate enhanced security features early in the design process. This is consistent with the expectations in the NRC's Advanced Reactor Policy Statement that, "advanced reactor designers should consider the expectations in the policy statement to ensure that security and emergency response are considered alongside safety during the early stages of plant design." The same policy statement goes on to say, "the Commission considers it prudent to provide expectations and guidance on security matters to prospective applicants so that they can use this information early in the design stage of new reactors to identify potential mitigative measures and/or design features that provide a more robust and effective security posture."

It is anticipated that rulemaking will be necessary in order to establish a consequence-based regulatory framework for SMRs and other new technologies. For near-term applicants, rulemaking may not be timely, and exemption requests would likely be necessary. However, initiating development of the technical basis to support a rulemaking would also support these near-term applicants and provide an efficient means to establish clarity and maintain consistency between the rulemaking and consideration of the associated exemption requests. Many of these applicants would like to incorporate concepts of the consequence based security framework into their designs. SMR applications are currently being developed, with the first design certification application anticipated to be submitted in late 2016, and the first combined license application anticipated to be submitted in late 2017 or early 2018.