NIMA ASHKEBOUSSI
Director, Fuel Cycle Programs

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8022
nxa@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 27, 2017

3/13/2017
82 FR 13511
1

Ms. Cindy Bladey
Office of Administration
Mail Stop: OWFN-12H08
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Comments on Security Design Considerations Preliminary Draft Guidance (Docket ID NRC-2017-0073)

Project Number: 689

Dear Ms. Bladey:

On behalf of the Nuclear Energy Institute's[1] (NEI) members, we appreciate the opportunity to comment on the Nuclear Regulatory Commission's (NRC) preliminary draft guidance on non-light water reactor (non-LWR) security design considerations (Docket ID NRC-2017-0073). The stated purpose of this preliminary guidance is to outline a set of security design considerations that a designer should consider while developing the facility design such that security issues can be effectively resolved through facility design, engineered security features, formulation of mitigation measures, and reduced reliance on human actions. Attached are general and specific comments on the draft guidance.

Small modular reactors (SMRs) and advanced non-LWRs will have significantly enhanced safety and security performance as compared to the reactors in operation today, including some designs utilizing fuel that is not susceptible to overheating and core damage. These technologies are capable of significantly lowering the risk of radiological sabotage, while reducing, or eliminating, the reliance on human actions. While we appreciate the NRC's attempt to provide designers information on incorporating security by design to meet regulatory requirements, as currently drafted the preliminary security design considerations only provide an overview of the existing regulatory requirements in 10 CFR Part 73. These regulations are intended for large light water reactors and do not provide new information or innovative guidance that recognizes the unique attributes of advanced reactors. Industry needs regulations and guidance that is appropriately framed for SMRs and non-LWRs.

[1] The Nuclear Energy Institute (NEI) is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

NEI submitted a White Paper[2] to propose new physical security requirements that are more appropriate for advanced reactor technologies. These proposals would continue to provide assurance that activities are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. We respectfully suggest that NRC prioritize rulemaking to support the changes identified in the White Paper. Such action would provide a greater benefit to industry, enabling plant designers to incorporate enhanced security features early in the design process that meet new regulatory requirements, rather than using the preliminary security design considerations (based on regulations for large light water reactors) as currently drafted.

NRC intends to incorporate the security design considerations with advanced reactor design criteria under one guidance document. In light of the future rulemaking, a better utilization of industry and NRC resources would be directed towards rulemaking and new guidance development, as opposed to developing security design considerations that fit into existing regulations. If the staff continues towards the development of security design considerations, it should do so in a coordinated manner with the NEI White Paper, where the considerations and guidance are based on advances achieved through the rulemaking process.

Thank you for your consideration of these comments. We look forward to remaining engaged on right-sizing the security requirements for advanced nuclear power generation technologies.

Please contact me if you have any questions.

Sincerely,

Nima Ashkeboussi

Nima Ashkeboussi

Attachment

c: Mr. George Tartal, NRO/DEIA, NRC
Mr. John Monninger, NRO/DSRA, NRC

[2] December 14, 2016, Letter from Pamela Cowan, NEI, to Vonna Ordaz, NRC, "Proposed Physical Security Requirements for Advanced Reactor Technologies"

Comments on Draft Security Design Considerations

Affected Section	Comment/Basis	Recommendation
1. General	The purpose of this draft document is unclear with respect to its application to advanced reactors. Part 73 was developed to apply to large LWRs. This draft guidance summarizes some existing regulations and some regulatory guides and does not offer non-LWR approaches to meeting security regulations. This draft document selectively addresses provisions of Part 73 for security considerations in the design of advanced reactors without an explanation of why the selective provisions are especially applicable to advanced reactor design. It would seem that the current design and licensing application process for identifying the security requirements, in accordance with Part 73 would be applicable for both LWRs and non-LWRs.	Recommend elaborating further on the NRC's intent behind this draft document.
2. General	The document describes the draft security design criteria as being applicable for advanced reactors. It appears that the same criteria could apply to small modular reactors. Is there a rationale for the criteria to not be applicable to SMRs?	Revise the document applicability to include SMRs.
3. General	IAEA is developing a draft guideline called "Security for the Lifetime of a Nuclear Facility." It sets international standards for security to be incorporated into the concept, design, layout, and construction of the facility.	Staff should consider any relevant guidelines for consideration. It can be found at www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst051.pdf

4. General	The Commission policy statement within 73 FR 60612 states, in part, "For new nuclear power reactors, 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 mitigated measures and/or design features that provide a more robust and effective security posture." Although the Commission supports guidance with regard to security for advanced reactors, the policy statement is not prescriptive as to what regulatory vehicle the NRC staff should use to offer guidance to potential applicants.	Consider deleting this draft guidance and re-issuing as information only through the use of a NUREG, or other regulatory vehicle, as appropriate.
5. General	This draft guidance makes statements such as, "These considerations, if adequately implemented through detailed design, along with the adequate implementation of administrative controls and security programs, are one way to protect a nuclear power reactor against the DBT for radiological sabotage". The NRC should clearly identify the *specific* regulation(s) that would be met by following/committing to this future regulatory guide.	Staff should clearly link each design consideration to a regulation and be clear that implementing the considerations satisfies the regulations.
6. General	In response to comment UCS-1 within the Commission policy statement contained in 73 FR 60615, the NRC response is as follows, "The GDC establish minimum requirements for the principal design criteria for nuclear power plants. The goal of the policy statement is not to raise these minimum requirements, but rather to encourage advanced reactor designers to consider safety and security matters during the development of future reactor designs. No changes were made to the policy statement as a result of this comment." This draft guidance leaves the impression that the security design considerations may be issued as part of the ARDC regulatory guide, which would raise the minimum requirements. This action would be counter to NRC response in the Commission policy statement.	Remove this draft guidance from the ARDC regulatory guidance to maintain separation between these security considerations.

7. General	In Section III, "Final Policy Statement," within 73 FR 60615, the Commission stated, in part, "Designs that 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." This bullet point underlines the inherent safety of advanced reactor designs, with their characteristic of reduced reliance on human action to maintain safety to the public and the environment. In contrast, this draft guidance continues to prescribe human action to mitigate unusual events when it may not be necessary to have any human action to resolve an event.	Consider relaxing human action requirements within the security design considerations. Any necessary actions could be demonstrated to be possible from remote locations, with the collaboration of the local law enforcement organizations, without having the necessity of a full onsite security team.
8. General	This draft guidance discusses different avenues for advanced reactors to undertake, but does not discuss standard design approvals (SDAs).	State the implication of this draft guidance on SDAs.
9. "NRC Policy on Advanced Reactors – Security" Section	The draft guidance states, "The integration of safety and security...," which is listed under an "NRC Policy" section. NRC policy is Commission policy, as denoted in the first paragraph of this section. The second paragraph of the section was written by the NRC staff. Therefore, it is misleading to place that paragraph in this section without further clarification.	Clarify that this definition of integration of safety and security is the NRC staff's interpretation, not Commission Policy.
10. "Security Design Considerations for Non-Light Water Reactors", 1st paragraph	This paragraph describes that this draft guidance contains security design considerations, but provides no definition for the term "considerations". "Considerations" is not a commonly used term by the NRC and the intent of this term is unclear. However, this paragraph states that considerations "should" be taken into account without any regulatory backing.	Clarify what is meant by the term "considerations," and the regulatory impact on applicant and licensees.

11. "Security Design Considerations for Non-Light Water Reactors", 2nd paragraph	The paragraph states, in part, "To establish guidance for designers to identify opportunities for resolving security issues." This phrase is confusing. It is unclear what "security issues" are in this context.	Clarify or revise the quoted text.
12. "Security Design Considerations for Non-Light Water Reactors", 2nd paragraph	The paragraph states, in part, "...the NRC staff considered the requirements in 10 CFR Part 73 that are related to the design of..." Although Part 73 is the principal regulation for security for power reactors, it is not the only part of the Code being considered by advanced reactor designers. Some small-scale advanced reactors may be considering a hybridization of 10 CFR Part 73 and 10 CFR Part 37.	Consider deleting this draft guidance. Advanced reactor designers, as appropriate, will provide justification on how their designs will conform to 10 CFR Part 37 or Part 73, as applicable.
13. "Security Design Considerations for Non-Light Water Reactors", 2nd paragraph	The paragraph states, "The design considerations were informed by requirements in 10 CFR Part 73 as well as existing guidance." It is unusual for regulatory guides that are issued by the NRC to summarize other regulatory guides. Typically, a regulatory guide is one method that the NRC considers acceptable to meet a specific regulation. A regulatory guide is not a distillation of other regulatory guides. In addition to other regulatory guides, this draft guidance mostly considers 10 CFR Part 73, which is fairly prescriptive (unlike the GDCs, for example). It is unusual to issue guidance that does a high-level summary of a whole Part to the CFR. Issuing guidance that 1) summarizes other guidance and 2) summarizes certain sections from a part to the CFR, seems inappropriate.	This preliminary draft guide provides no new information and reiterates the existing regulatory requirements that are described in other regulatory guides. It's not clear what the need for this document is.
14. "Process" Section	It is unclear in what form these security design considerations will ultimately be published. The text gives the impression that they will be published as part of the ARDC RG.	Clarify on the intent and regulatory vehicle of publishing the security design considerations.

15. Item 1, Intrusion detection systems	The draft guidance provides a design consideration that reads "design of physical security structures, systems, and components relied on for interior and exterior intrusion detection functions." This text is unnecessarily wordy and maybe subject to misinterpretation because the scope of SSCs that are relied on for intrusion detection may be misinterpreted. The requirement text should focus on the detection system itself and be established at the system level. This suggestion aligns the requirement with current industry guidance for security ITAAC.	Revise sentence to read: "The design of interior and exterior physical security intrusion detection systems..."
16. Item 1, Intrusion detection systems	The draft guidance provides a design consideration that requires "detecting unauthorized access into vital and protected areas." The requirement should be the detection of attempted and actual unauthorized penetration. This suggestion aligns the requirement with current industry guidance for security ITAAC.	Revise sentence to read: "...should provide assurance of detecting attempted and actual unauthorized penetration of vital and protected area barriers."
17. Item 1, Intrusion detection systems	The draft guidance provides a design consideration that requires a system to detect "unauthorized access into vital and protected areas." This text is somewhat ambiguous since a barrier could be violated without someone achieving access. Suggest changing the term to "unauthorized penetration of vital and protected areas barriers." This suggestion aligns the requirement with current industry guidance for security ITAAC.	See comment 15 above.
18. Item 1, Intrusion detection systems	The draft guidance provides a design consideration that requires the intrusion detection system design to "apply the principle of diversity." The requirement for diversity is not contained in the regulations. Furthermore, the implementation of the term "diversity" may incur different interpretations regarding how a design should be diverse. The objective should be to design the system with multiple approaches to provide an integrated capability. This suggestion is consistent with wording in NUREG-1959.	Revise sentence to read: "The design should apply multiple methodologies to provide an integrated detection capability."

19. Item 1, Intrusion detection systems	The draft guidance provides a design consideration that requires "reliability and availability of systems and components to achieve the intended intrusion detection functions." 10 CFR 73.55(b) does not address reliability of equipment. Since probability analysis is not applied to the design of security systems the application of terms such as "reliability" can be ambiguous. Suggest removing this requirement as part of the changes suggested in comment 4.	See comment 17 above.
20. Item 2, Intrusion assessment systems.	The draft guidance provides a design consideration that requires "design of physical security structures, systems, and components relied on for intrusion assessment functions." This text is unnecessarily wordy and maybe subject to misinterpretation because the scope of SSCs that are relied on for intrusion assessment may be misinterpreted. The requirement should be established at the system level. This suggestion aligns the requirement with current industry guidance for security ITAAC.	Revise to read: "The design of physical security intrusion assessment systems..."
21. Item 2, Intrusion assessment systems	The draft guidance provides a design consideration that requires "diversity necessary for the reliability and availability of systems and components to achieve the intended intrusion assessment functions." It is unclear why diversity is necessary for intrusion assessment equipment. There is no underlying requirement for this design feature in the regulations. Furthermore, the implementation of the term "diversity" may incur different interpretations regarding implementing design requirements. Suggest revising the requirement to more closely align with current COL/DCD security ITAAC.	Revise to read: "...should provide visual displays and suitable annunciation of alarms in the central and secondary alarm stations."
22. Item 2, Intrusion assessment systems	"The design should apply the principle of diversity necessary for the reliability and availability of systems and components to achieve the intended intrusion assessment functions."	Even though redundancy is not mentioned, if a camera system is lost the other diverse systems do not provide the same intrusion detection time and therefore you are driven to redundancy.
23. Item 2, Rationale	The draft guidance states, "Engineered intrusion assessment systems...provides, at all times, the capability	Revise the wording "capability to assess unauthorized persons" to read "capability to detect

	to assess unauthorized persons...." This language, "capability to assess unauthorized persons," is incomplete with respect to the language in 10 CFR 73.55(i).	and assess unauthorized persons," consistent with 10 CFR 73.55(i)(1).
24. Item 3, Security communication systems	The draft guidance provides a design consideration that requires communications systems "provide assurance of continuity and integrity of communications. Communication systems should account for design basis threats that can interrupt or interfere with continuity or integrity of communications." This requirement is beyond anything that current LWR COL holders are required to meet, is not consistent with the latest COL/DCD ITAAC for physical security, and is beyond the requirements in 10 CFR 73.55(j). Suggest revising to more closely align with current COL/DCD physical security ITAAC.	Revise to read: "The central and secondary alarm stations are capable of continuous communication with security personnel, and have communications capability with the main control room and local law enforcement authorities. Non-portable communication equipment in the central and secondary alarm stations remains operable from an independent power source in the event of loss of normal power."
25. Item 4, Security delay systems	"The design of security delay systems should be appropriately layered for defense-in depth	This is not specific in what would satisfy this requirement. Each of the sections has this same type of high level language which is open to a wide range of interpretation.
26. Item 5, Security response	The draft guidance provides a design consideration title for item 5 as "Security response." This title does not correspond to the design of any particular equipment.	Revise to read: "Security response equipment."
27. Item 5, Security response	The design of engineered physical security structures, systems, and components performing neutralization functions and ***engineered fighting positions*** relied on to protect ***security personnel performing neutralization functions*** should provide ***overlapping fields of fire***. The design configuration should provide layers of opportunities for security response, with each layer assuring that a single failure does not result in the loss of capability to neutralize the design basis threat adversary."	The highlighted text implies that a non-LWR must have a security staff appropriately sized to engage a threat in similar fashion to the approach employed at conventional LWRs. Although the guidance identifies the potential use of remotely controlled weapons systems, a security approach based on assessment and delay until engagement coming from an offsite force must be considered given the small footprint, power output and associated staff numbers anticipated for these plants.

28. Item 6, Control measures protecting against land and waterborne vehicle bomb assaults.	The draft guidance provides a design consideration for protection from vehicle bombs for "the reactor building and structures containing safety related structures, systems, and components." This terminology is different than is typically used for security protection, which usually refers to "vital areas."	Replace the reference to "the reactor building and structures containing safety related structures, systems, and components" with "vital areas."
29. Item 6, Control measures protecting against land and waterborne vehicle bomb assaults.	The draft guidance discusses a design consideration to provide a "minimum safe stand-off distance to adequately protect all structures, systems, and components required for safety and security." This terminology is too ambiguous and is different than is typically used for security protection, which usually refers to "vital areas."	Replace the reference to "structures, systems, and components required for safety and security" with "vital areas."
30. Item 9, Cyber Security Defense in Depth.	The draft guidance discusses a "strategy consisting of complementary and redundant cyber security Controls" to be implemented to establish layers of protections to safeguard critical digital assets. Rather than discussing the addition of redundant cyber security controls, these considerations should encourage design that includes non-digital safety systems that can avoid the need to implement cyber security programs.	Identify considerations that designers use to avoid the need to implement NRC cyber security programs per 10 CFR 73.54. If non-digital assets provide redundancy, cyber security protections should not be regulatory requirements.