Preliminary Draft Guidance
Non-Light Water Reactor
Security Design Considerations

The Nuclear Regulatory Commission Regulatory Framework for Security

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," includes requirements for the security of power reactors. In 10 CFR 73.1(a), "Purpose," the U.S. Nuclear Regulatory Commission (NRC) requires the establishment and maintenance of a physical protection system that will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. In 10 CFR 73.1(a)(1), "Radiological sabotage," the NRC defines design basis threats (DBT) that shall be used to design safeguards systems to protect against acts of radiological sabotage.

In 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," the NRC includes physical protection requirements for nuclear power reactors. The performance-based requirements in 10 CFR 73.55(b), "General performance objective and requirements," require licensees to establish and maintain a physical protection program. Within the design of a physical protection program, a physical protection system, consisting of engineered systems that are integrated with administrative controls (people, processes, and procedures), must ensure that there are capabilities to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage as described in 10 CFR 73.1, "Purpose and scope." The NRC establishes the specifics of how certain engineered systems must be designed or configured (or both), along with program, process, and organization requirements, in subsections of 10 CFR 73.55. The design of a physical protection system must meet the requirements of 10 CFR 73.55, unless exemptions or alternatives are justified, in accordance with 10 CFR 73.5, "Specific exemptions," or 10 CFR 73.55(r), "Alternative measures," respectively.

In addition, 10 CFR 73.54, "Protection of digital computer and communication systems and networks," establishes a performance-based requirement to ensure that certain digital computer and communication systems and networks at nuclear power plants are adequately protected against cyber attacks, up to and including the DBT for radiological sabotage as described in 10 CFR 73.1.

The processes for a license, certification, or approval of a combined or operating license, design certification, or early site or construction permit, respectively, are in accordance with the requirements of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "License, Certifications, and Approvals for Nuclear Power Plants." Where designs of a nuclear power reactor will be certified under 10 CFR Part 52, Subpart B, "Standard Design Certifications," 10 CFR 52.48, "Standards for Review of Applications," provides that the NRC will review an application filed for compliance with the standards set forth in 10 CFR Part 73. Similarly, an application to operate a nuclear power reactor pursuant to requirements in 10 CFR Part 50 or 10 CFR Part 52, Subpart C, "Combined Licenses," must satisfy the applicable requirements in 10 CFR Part 73 for nuclear power reactors.

NRC Policy on Advanced Reactors—Security

The Commission's "Policy Statement on the Regulation of Advanced Reactors," (73 FR 60612; October 14, 2008) states 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."

The integration of safety and security should consider the effects of the design of physical security-related structures, systems, and components (SSCs) on safety-related SSCs and required operator actions, including emergency response. Similarly, the integration should account for the effects of the design of the nuclear power plant on the security-related SSCs and the required security response to achieve their functions. This integration includes the site layout and locations of safety-related SSCs and buildings.

Security Design Considerations for Non-Light Water Reactors

This document sets forth a set of security design considerations that a designer should consider while developing the facility design. The NRC staff is using the term "security design considerations" to distinguish them from the general design criteria (GDC) in 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants." The GDC establish minimum requirements for the principal design criteria for water-cooled nuclear reactors. There are no GDC for security in 10 CFR Part 50, Appendix A.

To establish guidance for designers to identify opportunities for resolving security issues through the facility design, engineered security features, formulation of mitigation measures, and reduced reliance on human actions, the NRC staff considered the requirements in 10 CFR Part 73 that are related to the design of engineered systems that provide key security functions for protecting a nuclear power plant against the DBT external assaults. The NRC staff then identified considerations significant for the design of systems to achieve their intended security functions. The design considerations were informed by requirements in 10 CFR Part 73 as well as existing guidance. Similarly, the design considerations identified for cyber security highlight the concepts a system architect or designer may consider in developing protection for digital computer and communication systems at nuclear power plants.

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. These considerations do not limit designers or applicants from applying other methods or approaches in designing engineered systems to perform intended security functions. Consistent with the Commission's "Policy Statement on the Regulation of Advanced Reactors," these considerations should be considered early in the design process.

Process

The NRC staff believes that obtaining public comments on this preliminary draft version will be beneficial. Therefore, the security design considerations, along with the NRC's initial rationale for each, are being made available for comment. After receiving and considering comments, the NRC staff intends to include the security design considerations in a guidance document that

is being developed for advanced reactor design criteria for non-light water reactors (non-LWRs). On April 7, 2016, the NRC issued the draft "Advanced Non-Light Water Reactor Design Criteria" (Agencywide Documents Access and Management System Accession No. ML16096A420) for a 60-day informal public comment period. These design criteria address the safety aspects of non-LWRs. The NRC staff intends that the guidance document will include both safety design criteria and security design considerations.

As part of this process, the NRC will make this draft guidance document available for public comment through a *Federal Register* notice. After receiving and considering public comments on the draft guidance, the NRC staff intends to issue a final document that will provide guidance to non-LWR applicants to use when developing appropriate principal design criteria for their facilities.

Please note that some of the referenced documents within the security design considerations are not publicly available because they contain safeguards information, security-related information, or other types of information that the NRC cannot release to the public.

Topics Open for Comment

The table below, "DRAFT Non-LWR Physical and Cyber Security Design Considerations –- March 2017," includes the specific information on which the NRC is seeking comment. The table consists of seven physical security design considerations (1-7) and three cyber security design considerations (8-10), along with the NRC staff's rationale for each consideration.

Additionally, the NRC is seeking comment on whether the scope of the security design considerations should be broader or narrower, based on the specifics of the designs of the non-LWR technologies under development. Commenters may also submit suggestions on general principles and good practices for designs of engineered SSCs to achieve physical and cyber security functions identified in the security design considerations.

Commenting Instructions

Please refer to the associated *Federal Register* notice for instructions on providing comments.

Paperwork Reduction Act Statement

This draft guidance document contains information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), approval number 3150-0002.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
1	*Intrusion detection systems*. The design of physical security structures, systems, and components relied on for interior and exterior intrusion detection functions should provide assurance of detecting unauthorized access into vital and protected areas. The design should apply the principle of diversity necessary for the reliability and availability of systems and components to achieve the intended intrusion detection functions. Rationale Engineered intrusion detection systems (internal and external) are relied on for detecting unauthorized access into vital and protected areas. The initiation of plant security response begins and is based on this critical detection element of a physical protection system. A design that is reliable and available can provide assurance that intrusion detection functions can address the performance-based regulatory requirements of 10 CFR 73.55(b), "General performance objective and requirements." In addition, 10 CFR 73.55(i), "Detection and assessment systems," addresses the establishment and maintenance of intrusion detection systems that satisfy the requirements of 10 CFR 73.55(b) and provide, at all times, the capability to detect unauthorized persons and to facilitate the effective implementation of the licensee's protective strategy. The design considerations are informed by guidance found in, but not limited to, Regulatory Guide (RG) 5.44, "Perimeter Intrusion Alarm Systems"; RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued March 2011; NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980; NUREG/CR-4298, "Design and Installation of Computer Systems to Meet the Requirements of 10 CFR 73.55," issued July 1985; NUREG/CR-1468, "Design Concepts for Independent Central Alarm Station and Secondary Alarm Station Intrusion Detection Systems," issued in 1980; SAND99-2388, "Technology Transfer Manual—Interior Intrusion Detection," issued in 1999; SAND99-2390, "Technology Transfer Manual—Alarm Communication and Display," issued September 1999; and SAND99-2391, "Technology Transfer Manual—Exterior Intrusion Detection," issued August 1999.
2	*Intrusion assessment systems.* The design of physical security structures, systems, and components relied on for intrusion assessment functions should provide assurance of rapid remote assessment for determining cause and initiating appropriate security responses. 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. Rationale Engineered intrusion assessment systems are relied on by security personnel to assess intrusion alarms for unauthorized access into vital and protected areas. The implementation of required plant security response relies on information provided by these systems for protecting the nuclear power reactor against malevolent acts. A design that is reliable and available can provide assurance that assessment functions can address the performance-based regulatory requirements of 10 CFR 73.55(b). In addition, 10 CFR 73.55(i) addresses the establishment and maintenance of an assessment system that satisfies the design requirements of 10 CFR 73.55(b)

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
	and provides, at all times, the capability to assess unauthorized persons and facilitate the effective implementation of the protective strategy. The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued March 2011; NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980; and SAND99-2390, "Technology Transfer Manual—Alarm Communication and Display," issued September 1999.
3	*Security communication systems.* The design of structures, systems, and components (e.g., dedicated or plant operations systems) relied on for security communications should 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. The design should apply the principles of redundancy and diversity. Rationale Engineered systems for communications (e.g., dedicated or plant operations systems) are relied on for coordinating the security response to the design basis threat onsite and to request offsite assistance. A design that is reliable and available can provide assurance that communication functions can address the performance-based regulatory requirements of 10 CFR 73.55(b). In addition, 10 CFR 73.55(j), "Communication requirements," addresses the establishment and maintenance of continuous communications capabilities with onsite and offsite resources to ensure effective command and control during both normal and emergency situations. The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued March 2011; NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980; SAND99-2390, "Technology Transfer Manual—Alarm Communication and Display," issued September 1999; and SAND99-2392, "Technology Transfer Manual—Protecting Security Communications," issued August 1999.
4	*Security delay systems.* The design of structures, systems, and components relied on for delay functions should provide assurance for security responses to adversary attacks. The design of security delay systems should be appropriately layered for defense-in-depth. Rationale Engineered structures, systems, and components are relied on to delay an adversary which provides security responders opportunities to interdict or neutralize the design basis threat adversary. Sufficient delay times achieved by design of delay barrier systems and plant configurations enable security responses to interrupt adversaries from completing tasks for radiological sabotage.

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
	This can provide assurance that the security response functions can address the performance-based regulatory requirements of 10 CFR 73.55(b). In addition, 10 CFR 73.55(e)(1)(i), "Physical barriers," addresses the design, construction, installation and maintenance of physical barriers necessary to control access into physical areas for which access must be controlled or denied to satisfy the physical protection program design requirements of 10 CFR 73.55(b). The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980; SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," issued September 2007; and "SAND2001-2168, "Technology Transfer Manual—Access Delay Manual," Volume I, issued August 2001.
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. Rationale Engineered structures, systems, and components are relied on to protect security responders performing neutralization functions. Engineered remotely-controlled weapon platform systems capable of neutralization functions are a means of reducing reliance on human actions (i.e., security staff). A design that is reliable and available can provide assurance that engineered systems relied on for security responses can address the performance-based regulatory requirements of 10 CFR 73.55(b). In addition, 10 CFR 73.55(k), "Response requirements," addresses the establishment and maintenance, at all times, of properly equipped personnel to interdict and neutralize threats up to and including the design basis threat of radiological sabotage to prevent significant core damage and spent fuel sabotage. The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; RG 5.54, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants"; NUREG/CR-0543, "Central Alarm Station and Secondary Alarm Station Planning Document," issued June 1980; SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," issued September 2007; "SAND2001-2168, "Technology Transfer Manual—Access Delay Manual," Volume I, issued August 2001; and IROW-002, "Performance Specification System Specifications for the Interagency Remotely Operated Weapon Systems (IROWS)".
6	*Control measures protecting against land and waterborne vehicle bomb assaults*. The design of physical security structures, systems, and components, in conjunction with site-specific natural features, that are relied on to protect against a design basis threat land vehicle and waterborne vehicle bomb assault should provide assurance for the protection of the reactor building and structures containing safety related structures, systems, and components from explosive effects that are based on the maximum design basis threat quantity of explosives. The vehicle control measures (passive and active barrier systems) to deny land or waterborne vehicle

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
	bomb assaults should be located at a bounding minimum safe stand-off distance to adequately protect all structures, systems, and components required for safety and security. Rationale Engineered physical barriers (active and passive systems) are relied on to protect the reactor, the spent fuel pool, and other systems, structures, and components against the design basis threat land vehicle and waterborne vehicle bomb assaults. A design that is reliable and available can provide assurance for protection against vehicle bomb assaults that can address the performance-based regulatory requirements of 10 CFR 73.55(b). Consistent with the physical protection program design requirements of 10 CFR 73.55(b), and in accordance with a site-specific analysis, 10 CFR 73.55(e)(10), "Vehicle control measures," addresses the establishment and maintenance of vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage vehicle bomb assault. The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; NUREG/CR-6190, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants," issued December 1994; U.S. Army Corps of Engineers (USACE), "Update of NUREG/CR-6190 to Reflect Revised Design Basis Threat"; USACE PDC-TR-06-05, "Evaluating Adequacy of Landform Obstacles as Vehicle Barriers"; USACE PDC-TR-06-06, "Passive Inertial Vehicle Barrier Design Guide"; and USACE PDC-TR-06-09, "Vehicle Access Control Point Guidance."
7	*Access control portals:* The design of access control portals should provide assurance of detecting and denying unauthorized access to persons and pass-through of contraband materials (e.g., weapons, incendiaries, explosives). The design should apply the principles of redundancy and diversity to achieve the intended control functions. Rationale Engineered structures, systems, and components at the access control portals are relied on to detect and deny unauthorized persons and material into the protected area. The access portal is also integral to protecting against the design basis threat adversary assault. The capability to reliably detect and prevent unauthorized persons and material at the access control portals is integral to the protection against the design basis threat. A design that is reliable and available can provide assurance that access control functions can meet the performance-based regulatory requirements of 10 CFR 73.55(b). In addition, 10 CFR 73.55(g), "Access controls," addresses the control of personnel, vehicle, and material access at each access control point in accordance with the physical protection program design requirements of 10 CFR 73.55(b). The design considerations are informed by guidance found in, but not limited to, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors"; USACE PDC-TR-06-09, "Vehicle Access Control Point Guidance;" SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual;" and SAND2001-2168, "Technology Transfer Manual—Entry Control and Contraband Detection System."

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
8	*Defense model architecture.* The design of the defensive architecture for digital systems and networks to protect against a cyber attack should establish the logical and physical boundaries between digital assets with similar risks and digital assets with lower security risks. Digital assets associated with safety, important to safety, and security functions should be located at the highest security level and protected from all lower levels. Rationale Segmentation of the cyber-related network architecture will minimize the method and level of access to critical digital computer and communication systems. Under 10 CFR 73.54(c)(4), the cyber security program must be designed to ensure that the function of protected assets identified in 10 CFR 73.54(b)(1) is not adversely impacted due to cyber attacks. The design considerations are informed by guidance found in, but not limited to, Section C.3.2.1, "Security Defensive Architecture," of RG 5.71, "Cyber Security Programs for Nuclear Facilities"; and Section 5.1, "Network Segmentation and Segregation," of National Institute of Standards and Technology (NIST) SP-800-82, "Guide to Industrial Control Systems Security," Revision 2.
9	*Cyber security defense-in-depth.* A defense-in-depth protective strategy consisting of complementary and redundant cyber security controls should be employed to establish layers of protections to safeguard critical digital assets, critical systems, or both. The failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function. Rationale A layered strategy involving different overlapping security mechanisms can minimize the impact of a failure in any one mechanism. Under 10 CFR 73.54(c)(1) and 10 CFR 73.54(c)(2), the cyber security program must be designed to implement security controls to protect the assets identified by 10 CFR 73.54(b)(1), and to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks. The design considerations are informed by guidance found in, but not limited to, Section C.3.2, "Defense-in-Depth Protective Strategies," of RG 5.71, "Cyber Security Programs for Nuclear Facilities"; and Section 5.6, "Recommended Defense-in-Depth Architecture," of NIST SP-800-82, "Guide to Industrial Control Systems Security," Revision 2.
10	*Least functionality.* The design of the digital assets and digital communication systems should incorporate the principle of least functionality. The design should: (1) Eliminate unused/unnecessary functionality, protocols, ports, and services capable of being used in a stage of a cyber attack; or (2) Disable unused/unnecessary functionality, protocols, ports, and services and provide protections against enabling and use of the capabilities in a stage of a cyber attack; or

	VIII. Security
No.	**Security Design Consideration Language/Rationale**
	(3) Provide protections to prevent the use of unused/unnecessary functionality, protocols, ports, and services in a stage of a cyber attack when eliminating or disabling the capabilities is not practical. Rationale Least functionality helps to minimize the potential for introduction of security vulnerabilities, which are exploited in cyber attacks. Incorporating least functionality also reduces the volume of data to be monitored to determine if the asset or critical system is in a secure state. In 10 CFR 73.54(b)(1), the NRC requires an analysis of digital computer and communication systems and networks and identification of those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a). Under 10 CFR 73.54(c)(4) the cyber security program must be designed to ensure that the functions of protected assets identified in 10 CFR 73.54(b)(1) are not adversely impacted due to cyber attacks. A design that incorporates the principles of least functionality can reduce the number of protection mechanisms needed and make it easier to verify the security posture of the system. The design considerations are informed by guidance found in, but not limited to, Section C.11.8, “Least Functionality,” of RG 5.71, “Cyber Security Programs for Nuclear Facilities”; and Control SA-15(5), “Development Process, Standards, and Tools | Attack Surface Reduction,” of NIST SP-800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4.