



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

January 6, 2022

Mr. George J. Galatis  
4037 Shorewood Dr.  
Pensacola, FL 32507-8111

Dear Mr. Galatis:

We received your concerns related to the safety of spent fuel pools and, specifically, the ability of an adversary to drain water from the pool, exposing heated fuel to air that results in a fire and subsequent spread of contamination. The information below provides specific regulatory requirements that address spent fuel pool sabotage, the programmatic and inspection-related activities to verify compliance with those requirements, and technical information and analyses of spent fuel pools.

### **Regulatory Requirements**

In accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(b)(3), “[t]he physical protection program must be designed to prevent significant core damage and spent fuel sabotage.” Radiological sabotage with respect to spent fuel can be caused by a loss of spent fuel pool water inventory and subsequent exposure of spent fuel, thereby creating the potential for the release of fission products. The U.S Nuclear Regulatory Commission (NRC) performed analyses and developed guidance and inspection procedures (IPs) to ensure effective implementation of the above requirement, although due to the nature of this topic, most of the specific technical and programmatic information has been designated as official use only Security-Related Information (OUO-SRI) or Safeguards Information (SGI).

### **Programmatic and Inspection-Related Activities**

NRC inspectors use IP 71130.05, “Protective Strategy Evaluation and Performance Evaluation Program,” to verify that licensees develop, implement, and maintain a performance evaluation program that describes and demonstrates assessment of the effectiveness of the onsite physical protection program and protective strategy.

In addition, NRC inspectors use IP 71130.03, “Contingency Response – Force-on-Force Testing (OUO-SRI),” to assess each licensee’s physical protection program to ensure that it has been appropriately developed, designed, and implemented to protect target set equipment and prevent significant core damage and spent fuel sabotage from the design-basis threat of radiological sabotage in accordance with 10 CFR 73.1, “Purpose and Scope;” 10 CFR 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage;” and 10 CFR 73.58, “Safety/security interface requirements for nuclear power reactors.” This is a triennial inspection of an NRC-evaluated force-on-force exercise where a licensee can demonstrate the ability to implement its physical protection program.

**Technical Information/Analyses**

Staff has conducted studies to assess the risk associated with spent fuel pools, including risk from security events, and concluded that, with the regulatory measures in place, the risk associated with spent fuel pools is within the Commission's safety goal policy. In particular, the U.S. Army Corps of Engineers Protective Design Center Technical Report PDC-NRC-14-01 (SGI), dated May 2014, provides an approach the NRC finds acceptable for licensees to assess damage of spent fuel pools from sabotage threats.

In conclusion, there is agreement that maintaining integrity of the spent fuel pool and preventing spent fuel pool sabotage are important aspects to consider in the design of a licensee's physical protection program. The NRC has specific regulatory requirements for spent fuel pool sabotage and verifies compliance with these requirements. Additionally, studies have been conducted to verify that the risk associated with spent fuel pools, including risk from security events, is within the Commission safety goal policy.

Please feel free to contact me by email at [Todd.Keene@nrc.gov](mailto:Todd.Keene@nrc.gov) or by phone at (301) 287-0790.

Sincerely,



Signed by Keene, James  
on 01/06/22

J. Todd Keene, Chief  
Security Oversight and Support Branch  
Division of Security Operations  
Office of Nuclear Security and Incident Response