OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE

REGULATORY AUDIT TOPICS

REGARDING CYBER SECURITY DESCRIBED IN

OPERATING LICENSE APPLICATION

CONSTRUCTION PERMIT NO. CPMIF-001

SHINE MEDICAL TECHNOLOGIES, LLC

SHINE MEDICAL ISOTOPE PRODUCTION FACILITY

DOCKET NO. 50-608

By letter dated July 17, 2019 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML19211C044 as supplemented by letters dated November 14, 2019 (ADAMS Accession No. ML19337A275), March 27, 2020 (ADAMS Accession No. ML20105A295), August 28, 2020 (ADAMS Accession No. ML20255A027), November 13, 2020 (ADAMS Accession No. ML20325A026), December 10, 2020 (ADAMS Accession No. ML20357A084), and December 15, 2020 (ADAMS Accession No. ML21011A264), and March 23, 2021 (ADAMS Accession No. ML21095A235), SHINE Medical Technologies, LLC (SHINE) submitted to the U.S. Nuclear Regulatory Commission (NRC) an operating license application for its proposed SHINE Medical Isotope Production Facility in accordance with the requirements contained in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities."

During the NRC staff's review of the SHINE operating license application, questions have arisen related to SHINE's cyber security protections for which additional information is needed to determine that there is reasonable assurance of adequate protection of public health and safety and that applicable regulatory requirements are met. The topics below identify areas where additional information is needed for the NRC staff to continue its review of the SHINE cyber security protections and may become formal requests for additional information following the regulatory audit.

Regulatory Basis

The SHINE cyber security protections, as described in the SHINE operating license application, are being evaluated using the following regulations and guidance:

- Paragraph (b) of 10 CFR 50.34, "Contents of applications; technical information," states, in part, that "[t]he final safety analysis report [FSAR] shall include information that describes the facility, presents the design bases and the limits on its operation, and presents a safety analysis of the structures, systems, and components and of the facility as a whole…." As part of presenting its design bases, SHINE has established the following design criteria, summarized below, in its FSAR relevant to cyber security protections for safety systems (see: FSAR Section 7.4.2.2.1, "Access Control," for the Target Solution Vessel Reactivity Protection System (TRPS) criteria and FSAR

Section 7.5.2.2.1, “Access Control,” for the Engineered Safety Features Actuation System (ESFAS)):

- TRPS and ESFAS Criterion 2

  Development phases for ESFAS and TRPS software shall address the potential cyber security vulnerabilities (physical and electronic) to prevent unauthorized physical and electronic access.

- TRPS and ESFAS Criterion 3

  The ESFAS and TRPS design shall incorporate design or administrative controls to prevent/limit unauthorized physical and electronic access to critical digital assets (CDAs) during the operational phase, including the transition from development to operations. CDAs are defined as digital systems and devices that are used to perform or support, among other things, physical security and access control, safety-related functions, and reactivity control.

- Paragraph (d) of 10 CFR 73.67, “Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance,” includes requirements for fixed sites to control access to special nuclear material of moderate strategic significance. Licensees incorporating digital computer and communication systems and networks to implement their access control requirements should have cyber security controls to ensure these systems can perform their intended functions in the event of a cyber attack.

- Paragraph (a)(6) of 10 CFR 50.57, “Issuance of operating license,” states that an operating license may be issued upon finding, in part, that “[t]he issuance of the license will not be inimical to the common defense and security or to the health and safety of the public.”

Audit Topics

Audit Topic 1

FSAR Sections 7.4.2.2.1 and 7.5.2.2.1 include criteria to prevent unauthorized physical and electronic access to CDAs in safety systems during the operational phase and during transition from development to operations. Section 7.4.5.3.2, “Cyber Security Design Features,” of the SHINE FSAR provides a description of the SHINE cyber security design for the safety systems, including references to the defensive system architecture, communication via one-way isolated channels, requirements for use of a maintenance workstation, and no remote access capabilities. The NRC staff would like to understand the details of this implementation at the SHINE facility.

The NRC staff requests that SHINE provide a detailed description on how it will implement and maintain the cyber security requirements as set forth in the FSAR sections identified above. The information is necessary for the NRC staff to determine how SHINE is satisfying Design Criteria 2 and 3 for TRPS and ESFAS.

Audit Topic 2

The physical security plan provides a description of the measures used to protect the facility and ensure the Category 2 material is secure including some of the digital computer and communication systems and networks used. However, it is unclear if any cyber security protections have been implemented to ensure these systems can perform their intended functions in the event of a cyber attack.

The NRC staff requests that SHINE provide a detailed description of the cyber security protections that will be in place for the physical security systems to ensure that the access controls requirements of 10 CFR 73.67(d) are met, as well as how SHINE will implement and maintain these protections to meet 10 CFR 50.57(a)(6).