12.4.14 Cybersecurity

There are currently no NRC regulations regarding cybersecurity that apply to non-power production and utilization facilities intending to produce molybdenum-99 (Mo-99) like the SHINE facility. Therefore, in "Staff Requirements – SECY-18-0063 – Response to Staff Requirements Memorandum (SRM)-COMSECY-17-0008 on Physical Protection for Non-Power Production and Utilization Facilities Intending to Produce Molybdenum-99," dated September 26, 2019, the Commission directed the NRC staff to address cybersecurity at these facilities through subsequent development of appropriate license conditions based on the facilities' operating license applications. The staff determined that the best approach to develop such risk-informed site-specific license conditions to establish an adequate level of protection for the SHINE facility would be to use, as a starting point, the cybersecurity requirements for similar types of facilities.

The NRC staff reviewed the SHINE FSAR to determine if it includes an adequate level of cybersecurity protections to ensure that, in accordance with 10 CFR 50.57(a)(6), the issuance of an operating license for the SHINE facility will not be inimical to the common defense and security or to the health and safety of the public. The staff also performed a regulatory audit to determine what cybersecurity practices are being applied at the SHINE facility. The staff issued RAIs to SHINE to help gather further information, to which SHINE provided responses (ADAMS Accession No. ML21315A003). After completing this review, the staff determined that additional cybersecurity program elements were needed to provide reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks.

To ensure adequate protection at the SHINE facility, and consistent with SRM-SECY-18-0063, the NRC staff drew upon its review of the SHINE FSAR and lessons learned from the cybersecurity programs at nuclear power reactor facilities and the draft fuel cycle facility cybersecurity rulemaking (ADAMS Accession No. ML17018A218) to develop a list of important cybersecurity program elements applicable to the SHINE facility. These elements are included in the below risk-informed license condition that allows SHINE to apply a graded approach to cybersecurity based on the consequences of concern specific to the SHINE facility. The term "consequences of concern" is explained below. Specifically, the license condition requires SHINE to have a cybersecurity plan (CSP) that describes how the facility's cybersecurity program provides reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks. The license condition also requires that the cybersecurity program elements described in the CSP include the elements determined by the staff to be important and applicable to the SHINE facility. The staff determined that this license condition, in addition to the supplemental information provided by SHINE that is discussed immediately below, will ensure, in part, that the issuance of the operating license will not be inimical to the common defense and security or to the health and safety of the public. Therefore, the issuance of a SHINE operating license, as conditioned, in part, by the below license condition, meets the requirements of 10 CFR 50.57(a)(6).

On July 6, 2022, SHINE submitted a revision to its responses to RAIs related to cybersecurity (ADAMS Accession No. ML22223A066) that provides information regarding the design, administrative, and programmatic controls that the SHINE CSP will provide. This includes how consequences of concern will be identified, how critical digital assets (CDAs) will be determined, how cybersecurity controls will be applied, and other programmatic controls to ensure that the cybersecurity program is documented and maintained. The NRC staff determined that, through the combination of this information and the below cybersecurity license condition, once the SHINE CSP is implemented, there will be sufficient cybersecurity program elements in place to provide reasonable assurance that digital computer and communication systems and networks

are adequately protected against cyberattacks. The staff also reviewed the consequences of concern identified by SHINE in its July 6, 2022, revised responses to RAIs and determined that protecting CDAs associated with these consequences of concern provides reasonable assurance that issuance of the operating license will not be inimical to the common defense and security or to the health and safety of the public.

A consequence of concern is an event that occurs as a result of the compromise of a CDA that has the potential to adversely impact the public health and safety or the common defense and security. Licensees must identify and document those digital assets that, if compromised by a cyberattack, would result in a consequence of concern. Such digital assets that are then determined to be CDAs must be protected by the application of appropriate cybersecurity controls. A consequence of concern can be active or latent. In the case of an active consequence of concern, the compromise of the digital asset from a cyberattack directly results in a radiological or chemical exposure exceeding the safety criteria limits specified in a licensee's Final Safety Analysis Report. In the case of a latent consequence of concern, a digital asset is compromised but there is no direct impact on a safety, security, or safeguards function until a secondary event occurs (i.e., an initiating event separate from the cyberattack). The combination of the compromise of the digital asset from the cyberattack (i.e., the latent consequence of concern) and the secondary event must both occur for there to be a significant impact on public health and safety or common defense and security.

For facilities intending to produce Mo-99 such as the SHINE facility, the following consequences of concern must be considered (but may not necessarily apply):

Latent Safeguards: The concern involves the compromise as a result of a cyberattack of a digital asset performing a security function, which would allow a malicious actor to exploit the degraded security function that was put in place to prevent the unauthorized removal of SNM of moderate strategic significance or the loss of MC&A for SNM of moderate strategic significance.

Active Safety: In this situation, the cyberattack compromises the function of a digital asset and directly leads to safety-related consequences as defined in the safety criteria found in the licensee's Final Safety Analysis Report.

Latent Safety or Security: The attack renders one or more digital assets incapable of performing its intended function. When called upon to respond to an event, separate from the cyberattack, the digital asset does not operate as expected and therefore the supported safety or security function is compromised, resulting in safety-related consequences like above, or loss or unauthorized disclosure of classified information or classified matter. In addition, MC&A functions whose compromise could lead to a latent safety consequence of concern, would need to be protected from a cyberattack.

Based on the above, the SHINE operating license is conditioned as follows:

The licensee must have a cybersecurity plan (CSP) that describes how the facility's cybersecurity program provides reasonable assurance that digital computer and communication systems and networks are adequately protected against cyberattacks. The cybersecurity program elements described in the CSP must include but are not limited to the following:

1. Establishing a team with working knowledge in information and digital system technology, facility operations, engineering, safety, and the facility's physical security and emergency preparedness to identify the relevant consequences of concern, including latent safeguards, active safety, and latent safety or security

consequences of concern, as applicable, as defined in the NRC safety evaluation of the SHINE facility operating license application, and make informed cybersecurity decisions. Alternatively, establish equivalent individual roles and responsibilities in the CSP that ensure that informed cybersecurity decisions are made.

2. Identifying digital assets that, if compromised by a cyberattack, would result in a consequence of concern.
3. Determining which of these assets are critical digital assets (CDAs) that need to be protected to meet the cybersecurity program performance objectives of the facility.
4. Identifying a set of cybersecurity controls for CDAs and applying them so that there is reasonable assurance that the facility is adequately protected against cyberattacks.
5. Implementing site-specific defense-in-depth protective strategies that ensure that the failure of a single protective strategy or security control will not result in a consequence of concern by describing how the licensee delays, detects, prevents, responds to, and recovers from cyberattacks on CDAs, as applicable.
6. Providing temporary compensatory measures to meet the cybersecurity program performance objectives when the cybersecurity controls are degraded.
7. Establishing and maintaining a configuration management system to ensure that any changes to the facility are monitored and evaluated for potential cybersecurity impacts prior to implementation so that there is reasonable assurance that the facility is adequately protected against cyberattacks.
8. Periodically reviewing the effectiveness of the cybersecurity program to provide reasonable assurance that the cybersecurity program performance objectives of the facility are continuously met.
9. Tracking and reporting cybersecurity events.

The licensee may make changes to the CSP provided that the above cybersecurity program elements and the performance objectives of the CSP remain met and that these changes are made with the knowledge of the team, or its equivalent, of program element (1).