Revision 1 to Regulatory Guide 5.77, "Insider Mitigation Program": Regulatory Basis and Backfitting Assessment

INTRODUCTION:

Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," paragraph (b)(9) requires that licensees establish, maintain, and implement an insider mitigation program (IMP). The requirements of this program are set forth in 10 CFR 73.55(b)(9)(i)-(ii). Regulatory Guide (RG) 5.77, "Insider Mitigation Program," published in 2009, describes an approach that the U.S. Nuclear Regulatory Commission (NRC) staff considers acceptable for use in developing and implementing an IMP at a nuclear power reactor facility.

In Staff Requirements Memorandum (SRM)-M160623B, "Discussion of Security Issues," dated June 27, 2016 (Agencywide Documents Access and Management System Accession (ADAMS) No. ML16179A382), the Commission directed the NRC staff to complete interactions with stakeholders regarding any updates to RG 5.77 and submit them to the Committee to Review Generic Requirements (CRGR) for review. The staff was directed to provide to the Commission, for review and approval, the final revised RG, including a regulatory basis for the proposed revisions, as well as a documented evaluation or backfitting analysis, as applicable, in accordance with 10 CFR 50.109, "Backfitting." Since the proposed revisions in this RG are designed to clarify existing guidance and to provide an acceptable method by which licensees can meet 10 CFR 73.55(b)(9), the proposed revisions are not requirements. Consequently, this enclosure provides the regulatory basis and backfitting assessment rather than a backfitting analysis or documented evaluation.

Since issuance of RG 5.77 in March 2009, lessons learned from inspections, operating experience, and licensee interactions with staff have identified clarifications that are being incorporated into the guidance. The staff has identified two substantive areas needing clarification and included them in the proposed revision. They are:

- guidance on the specific elements of the fitness-for-duty (FFD) program in 10 CFR Part 26 that a licensee should choose to use to implement its IMP; and
- guidance on the cyber security provisions in 10 CFR 73.54 that a licensee should choose to use to implement its IMP.

On January 4, 2016, the staff transmitted proposed Revision 1 to RG 5.77 to stakeholders authorized to receive Official Use Only - Security-Related Information and opened a 60 day comment period.[1] Several closed meetings were held with authorized stakeholders, including the Nuclear Energy Institute (NEI) and Dr. Edwin Lyman of the Union of Concerned Scientists (UCS) (who has a clearance and provides perspectives as a member of the public), regarding the proposed revisions. The NRC staff received several rounds of oral and written comments that were mostly administrative and editorial in nature. The staff addressed these comments in the proposed final draft as applicable. After reviewing the final proposed revision of RG 5.77, NEI, by e-mail dated December 5, 2016 (ADAMS Accession No. ML17066A444), stated that the industry had no further comments or questions. In a conversation with the NRC staff on October 21, 2016, UCS indicated that it found the proposed changes reasonable.

[1] Since the document was Official Use Only – Security-Related Information, the draft was not made publicly available and was not noticed in the *Federal Register*.

1. Elements of the FFD program (Part 26) that a reactor licensee, including those licensees in decommissioning and subject to Part 73 requirements, should choose to include in its IMP:

In the proposed revision to RG 5.77, the staff identifies and clarifies those elements of a 10 CFR Part 26 FFD program that support the IMP required by 10 CFR 73.55(b)(9). This clarification can help licensees that implement the guidance ensure that individuals who maintain unescorted access authorization (UAA) are trustworthy and reliable and, therefore, do not represent an insider threat during decommissioning to cause spent fuel sabotage.[2] This is particularly important when a reactor enters decommissioning, since the Part 26 FFD program no longer applies once the NRC dockets a licensee's certifications under 10 CFR 50.82(a). However, licensees are still required to maintain an IMP under 10 CFR 73.55(b)(9).

The original publication of the final Part 26 rule "Fitness-for-Duty Programs" (54 FR 24468; June 7, 1989) documented a strong nexus between drug testing and trustworthiness and reliability. For example, in the final rule's statement of considerations (54 FR 24468), the Commission stated: "The general objective of this [FFD] program is to provide reasonable assurance that nuclear power plant personnel are reliable, trustworthy, and not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties." Further, the Commission stated that "[g]iven the addictive and impairing nature of certain drugs, while recognizing that the presence of drug metabolites does not necessarily relate directly to a current impaired state, the presence of drugs does strongly suggest the likelihood of past, present, or future impairment affecting job activities. In addition, the NRC believes that the reliability, integrity, and trustworthiness of persons working within nuclear power plants is important to assure public health and safety." These statements indicate that the 1989 final rule had at least two primary purposes: (1) preventing, identifying, and responding to human impairment in the workplace caused by the use of legal or illegal substances and (2) determining whether individuals are trustworthy and reliable, in part, by their abstinence from misusing legal substances and possession, sale, or use of illegal substances. These purposes were maintained, clarified, and enhanced in an amendment to the Part 26 rule in 2008 (73 FR 16966; March 31, 2008).

Part 26 also includes requirements that go above and beyond impairment and trustworthiness and reliability determinations. For example, Part 26 establishes: (1) protections for individuals from being falsely accused of drug or alcohol use (e.g., medical review officer reviews of drug testing requirements and an appeals process); (2) requirements to help ensure the validity and accuracy of drug and alcohol testing (e.g., laboratory audits and quality assurance specimen testing); and, (3) required sanctions for FFD policy violations to enable individuals to seek treatment and to prevent individuals from gaining or maintaining UAA without licensee adjudication of the identified FFD concern. The NRC staff finds that these requirements are not necessary to meet the purpose of the IMP, because they focus primarily on program integrity, due process, and worker protections rather than requirements that effectively contribute to the purpose of the IMP.

There are Part 26 requirements that could contribute to the IMP such as employee assistance program and fitness determinations (such as a psychological assessments) performed by

[2] Spent fuel sabotage is defined as a loss of spent fuel pool inventory and exposure of spent fuel, barring extraordinary actions by plant operators. NUREG-2033, "Glossary of Security Terms for Nuclear Power Reactors," March 2017.

trained and qualified Substance Abuse Experts. Based on this staff assessment, the proposed revisions to RG 5.77 clarify the Part 26 requirements that would effectively contribute to the purpose of an IMP.

A. Regulatory Basis:

Under 10 CFR 73.55(b)(9), a licensee is required to establish, maintain, and implement an IMP to monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining UAA to a protected or vital area, and to implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage or spent fuel sabotage. As required by 10 CFR 73.55(b)(9)(ii)(B), a licensee's IMP must contain elements from the FFD program described in Part 26 that support a defense-in-depth regulatory approach and can be used to inform the licensee's IMP. However, the regulations do not identify which elements of the FFD program should be included in the IMP. The initial version of RG 5.77 provided nominal clarification of this requirement.

Further, at the time RG 5.77 was initially published in 2009, the NRC staff did not explicitly consider the applicability of the 10 CFR 73.55(b)(9) provisions to a Part 50 power reactor licensee in decommissioning. Based on an interpretation of the requirements in 10 CFR 50.82, "Termination of license," and 10 CFR 26.3, "Scope," following the initial publication of RG 5.77, staff determined that Part 26 applies to a Part 50 reactor licensee only when that licensee is authorized to operate. As a result, the proposed revisions provide both operating and decommissioning nuclear power reactor facilities additional guidance as to which elements of the licensee's FFD program should be implemented to support the IMP.

B. Backfitting Assessment:

Licensees subject to 10 CFR Part 73, "Physical Protection of Plants and Materials," requirements are currently required to implement in their IMPs elements from the FFD program described in Part 26. Prior to this revision of RG 5.77, the guidance only focused on the conduct of drug and alcohol testing for the five test conditions: pre-access, random, for-cause, post-event, and follow-up. However, the staff had not detailed which additional elements of Part 26 the licensee should choose to meet the IMP requirement during decommissioning. Current operating experience with decommissioning reactors shows that they have maintained their full Part 26 FFD programs throughout decommissioning thereby resulting in unnecessary regulatory burden because licensees in decommissioning do not need to implement a full Part 26 program to meet the IMP requirement.

All licensees implement RG 5.77, Revision 0, through their commitment to NEI 03-12 in their security plans. NRC staff is issuing Revision 1 to RG 5.77 to clarify which elements of Part 26 should be implemented to satisfy the IMP requirement. The staff finds that this revision to RG 5.77 will reduce burden to licensees, as multiple elements of Part 26 that are more administrative in nature are not identified as essential to the IMP for the decommissioning plants. Adherence to Revision 1 of RG 5.77 will not be mandatory and the staff does not intend any imposition or backfitting of Revision 1 to RG 5.77. Licensees may choose to meet the provisions of the IMP requirements using another approach. Consequently, the NRC staff did not perform a backfit analysis or documented evaluation.

C. Stakeholder/NRC Staff Discussion:

The NRC staff engaged authorized industry stakeholders and the UCS multiple times on the revision to the RG. Initially, industry representatives expressed concern about the Part 26 related changes to the RG. However, during the August 25, 2016, authorized stakeholder meeting, the staff explained the nature of the current Part 26 requirement and the expectation that the new guidance appropriately addressed the operating and decommissioning stages of a nuclear power reactor facility lifecycle. The industry did not submit any further comments to the revised RG. In a December 5, 2016, e-mail, NEI confirmed that industry had no further comments on the draft RG 5.77. In a conversation with the NRC staff on October 21, 2016, UCS indicated that it did not have any specific comments for or against this revision to the guidance.

2. Elements of the Cyber Security Program that a reactor licensee should choose to include in its IMP, including those licensees in decommissioning and subject to Part 73 requirements:

The NRC issued the cyber security rule on March 27, 2009, as part of the larger Power Reactor Security Requirements rule (74 FR 13926). According to 10 CFR 73.55(b)(9)(ii)(C), the IMP must contain elements from the cyber security program described in 10 CFR 73.54. RG 5.77, issued at the same time as the rule, did not clarify which elements of the cyber security program in 10 CFR 73.54 should be included in the IMP. As part of its discussion of cyber security, Revision 1 to RG 5.77 clarifies those elements of the cyber security program that should be included in a licensee's IMP. This revision of the RG captures the key content from Security Frequently Asked Question (SFAQ) 10-05, "Information Technology (IT) Functions for the Critical Group" that addressed IT personnel and the IMP.

A. Regulatory Basis:

Per the requirement in 10 CFR 73.55(b)(9)(ii)(C), the IMP must contain elements from the cyber security program described in 10 CFR 73.54, "Protection of digital computer and communication systems and networks."

Licensee personnel who perform the job functions described in 73.56(i)(1)(v)(B)(1)-(5) must be trustworthy and reliable. This includes any individuals who have access to, extensive knowledge of, or administrative control over plant digital computer and communication systems and networks, as identified in 10 CFR 73.54. SFAQ 10-05 resolved which IT functions and positions should be included as part of the licensee's critical group (as defined in RG 5.77) to ensure consistent and effective implementation of 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants." These IT functions and positions should include plant network systems administrators and IT personnel who are responsible for securing plant networks

B. Backfitting Assessment:

After the issuance of 10 CFR 73.54 and 10 CFR 73.55, industry representatives submitted SFAQ 10-05 to engage staff as to which specific IT personnel would be subject to the IMP. The resolution to SFAQ 10-05 contained the NRC staff's clarification regarding which "IT personnel" should be subject to the IMP provisions and which IT functions and positions are to be included as part of the "critical group" to ensure consistent and effective implementation of 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants."

Consistent with this position, staff has made conforming clarifications to the RG and defined the term “IT personnel” in the Glossary of Revision 1 to RG 5.77. The staff is not establishing a new or changed position in this clarification, as the revision is consistent with the already-established staff position in SFAQ 10-05.

Licensee compliance with Revision 1 of RG 5.77 is not considered mandatory, and the staff does not intend any imposition or backfitting of RG 5.77. Licensees are free to meet the provisions of the IMP requirements using another approach. However, it is incumbent on licensees to demonstrate how cyber security elements are addressed in the IMP. The guidance contained in this RG is strictly voluntary and, therefore, is not a backfit under 10 CFR 50.109. Consequently, the NRC staff did not perform a backfit analysis or documented evaluation.

C. Stakeholder/NRC Staff Discussion:

The staff engaged authorized stakeholders from industry and the UCS multiple times on the revision to the RG. Industry did not submit any further comments on the revised RG after the last revision, dated September 9, 2016. UCS did not have any specific comments for or against the September 9, 2016, revision to the guidance.