U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE 5.77, REVISION 1

Issue Date: September 2022
Technical Lead: Brad Baxter and Mark Resner

INSIDER MITIGATION PROGRAM

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes an approach that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for an insider mitigation program (IMP) for nuclear power reactors that contain protected or vital areas. Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(b)(9) (Ref. 1) requires licensees to establish, maintain, and implement an IMP.

Applicable Rules and Regulations

- 10 CFR 50.34(c)(2) (Ref. 2) states, in part, that each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," must include a physical security plan with its application. 10 CFR 50.34(c)(3) states, in part, that the physical security plan must describe how the applicant will meet the requirements of 10 CFR Part 73, "Physical Protection of Plants and Materials."

- 10 CFR 50.82(a)(1)(i) requires that, when a power reactor licensee has determined to permanently cease operations, the licensee shall, within 30 days, submit a written certification to the NRC, consistent with the requirements of 10 CFR 50.4(b)(8).

- 10 CFR 52.79(a)(35) (Ref. 3) states, in part, that an applicant for a combined license shall submit a physical security plan describing how the applicant will meet the requirements of 10 CFR Part 73.

- 10 CFR 73.1(a) provides the design-basis threats that shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material.

Written suggestions regarding this guide or development of new guides may be submitted through the NRC's public Web site in the NRC Library at https://nrcweb.nrc.gov/reading-rm/doc-collections/reg-guides/, under Document Collections, in Regulatory Guides, at https://nrcweb.nrc.gov/reading-rm/doc-collections/reg-guides/contactus.html.

Electronic copies of this RG, previous versions of RGs, and other recently issued guides are also available through the NRC's public Web site in the NRC Library at https://nrcweb.nrc.gov/reading-rm/doc-collections/reg-guides/, under Document Collections, in Regulatory Guides. This RG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at https://www.nrc.gov/reading-rm/adams.html, under ADAMS Accession Number (No.) ML16342B024. The regulatory analysis may be found in ADAMS under Accession No. ML14002A294. The associated draft guide DG-5044 may be found in ADAMS under Accession No. ML14002A295, and the staff responses to the public comments on DG-5044 may be found under ADAMS Accession No. ML22152A224.

- 10 CFR 73.54, "Protection of digital computer and communication systems and networks," paragraph (a), requires that licensees provide high assurance[1] that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat, as described in 10 CFR 73.1, "Purpose and scope." This program contains elements that are needed to support the IMP required by 10 CFR 73.55(b)(9).

- 10 CFR 73.55(b)(7) states that licensees shall establish, maintain, and implement an access authorization program in accordance with 10 CFR 73.56, "Personnel access authorization requirements for nuclear power plants." Furthermore, 10 CFR 73.55(b)(9) states that the IMP must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area and 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 and spent fuel sabotage.

- 10 CFR 73.56 requires licensees to establish, implement, and maintain an access authorization program. This program contains elements that are needed to support the IMP required by 10 CFR 73.55(b)(9).

- 10 CFR 73.57(a) requires that licensees submit fingerprints for those individuals who will have access to safeguards information (SGI).

- 10 CFR Part 26, "Fitness for Duty Programs" (Ref. 4), states, in part that fitness for duty (FFD) programs must provide reasonable assurance that individuals are trustworthy and reliable as demonstrated by the avoidance of substance abuse; individuals are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause that in any way adversely affects their ability to safely and competently perform their duties; the workplaces subject to 10 CFR Part 26 are free from the presence and effects of illegal drugs and alcohol; and programs must provide reasonable measures for the early detection of individuals who are not fit to perform the duties that require them to be subject to the FFD program. This program contains elements that are needed to support the IMP required by 10 CFR 73.55(b)(9).

Related Guidance

- RG 5.66, "Access Authorization Program for Nuclear Power Plants" (Ref. 5), provides guidance on access authorization program requirements contained in 10 CFR 73.56 and 10 CFR Part 26. RG 5.66 also endorses Revision 3 of Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plants Access Authorization Program" (Ref. 6), which contains security-related information in accordance with 10 CFR 2.390(d)(1) and, therefore, is not publicly available. The NEI guide describes an approach that the NRC staff has found acceptable in meeting the requirements for an access authorization program.

[1] In Staff Requirements Memorandum (SRM) SRM-SECY-16-0073, Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the Commission stated that "the concept of 'high assurance' of adequate protection found in our security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate." (ML16279A345)

- RG 5.69, "Guidance for the Application of the Radiological Sabotage Design Basis Threat in the Design, Development, and Implementation of a Physical Security Program that meets 10 CFR 73.55 Requirements" (Ref. 7), contains SGI and is not publicly available. The RG provides guidance for mitigating the active insider and passive insider threat.

- RG 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 8), provides guidance to licensees on cyber protection measures.

- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors" (Ref. 9), contains SGI and is not publicly available. It provides guidance and describes approaches that the NRC staff has found acceptable for meeting the requirements of 10 CFR 73.55. If effectively implemented by licensees accounting for site-specific conditions, the approaches and examples described in this RG would satisfy the general performance objective of 10 CFR 73.55 for the topics addressed.

- NUREG 1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," Revision 1, issued September 2017 (Ref. 10), provides a detailed discussion of proximity sensors, which may be used as part of an IMP.

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50, 52, 73, and 26 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 numbers 3150-0011, 3150-0151, 3150-0002, and 3150-0146, respectively. Send comments regarding this information collection to the FOIA, Library and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB Reviewer at: OMB Office of Information and Regulatory Affairs (NEOB-10202 3150-0011, 3150-0151, 3150-0002, and 3150-0146), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW, Washington, DC, 20503; e-mail: oira.submission@omb.eop.gov.

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.

TABLE OF CONTENTS

B. DISCUSSION

Reason for Revision

The NRC is revising RG 5.77 to provide updated guidance for implementing an IMP that meets the requirements of 10 CFR 73.55(b)(9). This revision is based on industry and NRC staff insights gained from lessons learned from inspections, operating experience, and licensee interactions with the NRC staff.

In addition, this revision provides licensees with guidance for continuing to meet the requirements for an IMP following the licensee's determination to permanently cease operations and remove fuel from the reactor vessel in accordance with 10 CFR 50.82(a)(1).

Background

Once an individual has been granted unescorted access to protected and vital areas of a power reactor facility, preventing an adverse event becomes dependent, in part, on the effective implementation of the IMP. The IMP monitors the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to protected or vital areas. The program must contain elements from the licensee's access authorization program, FFD program, cybersecurity program, and physical protection program. The implementation of the licensee's IMP, in combination with other regulatory security requirements, minimizes the potential for an insider to adversely affect a licensee's capability to prevent significant core damage and spent fuel sabotage.

The licensee's access authorization program must provide high assurance that individuals described in 10 CFR 73.56(b)(1) and (b)(2) are trustworthy and reliable, such that they do not constitute an unreasonable risk to public health and safety or the common defense and security, including the potential to commit radiological sabotage. The licensee's FFD program must provide, in part, reasonable assurance that nuclear power plant personnel are trustworthy and reliable, as demonstrated by the avoidance of substance abuse, and that such personnel are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause that in any way adversely affects their ability to perform their duties safely and competently. The licensee's cybersecurity program must, as described in 10 CFR 73.54(a), provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat, as described in 10 CFR 73.1. The concurrent and integrated implementation of these programs provides protection that minimizes the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to physically protect licensed activities against radiological sabotage.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops safety requirements and safety guides for protecting people and the environment from harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA safety requirements and safety guides pursuant to the Commission's International Policy Statement (Ref. 11) and Management Directive and Handbook 6.6, "Regulatory Guides," dated May 2, 2016 (Ref. 12).

The staff considered the following IAEA safety requirements and guide in the development and update of the RG:

- IAEA Nuclear Security Series No. 8-G, "Preventive and Protective Measures against Insider Threats," Revision 1, issued 2020 (Ref. 13).

C. STAFF REGULATORY GUIDANCE

1. General Requirements

In accordance with 10 CFR 73.55, the licensee must establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. The physical protection program must protect against the design-basis threat of radiological sabotage in accordance with 10 CFR 73.1 and be designed to prevent significant core damage and spent fuel sabotage.

As set forth in 10 CFR 73.55(b)(9), nuclear power reactor licensees are required to establish, maintain, and implement an IMP. This IMP must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area. The IMP must implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, a licensee's capability to prevent significant core damage or spent fuel sabotage. Additionally, the IMP must contain elements of the access authorization program described in 10 CFR 73.56; the FFD program described in 10 CFR Part 26; the cybersecurity program described in 10 CFR 73.54; and the physical protection program described in 10 CFR 73.55.

An important focus for an IMP is the implementation of measures that control the licensee's personnel access to the following:

a. protected areas,
b. vital areas,
c. accessible target set elements or areas,
d. digital computers,
e. communication systems, and
f. computer networks associated with:
    (1) safety-related and important to safety functions,
    (2) security functions, and
    (3) emergency preparedness functions.

Insider threats present a unique problem for a physical protection system. Insiders could take advantage of their access rights, authority, and knowledge of a facility to understand, bypass, or defeat dedicated physical protection elements or other provisions (such as measures for safety or material control and accounting, including operating measures and procedures) to assist a potential adversary. Furthermore, personnel with access in positions of trust, such as those detailed in 10 CFR 73.56(i)(1)(v)(B), can carry out subversive actions not available to outsiders when confronted with protection elements and access controls.

Insiders have more opportunities to access safety- or security-significant structures, systems and components, select the most vulnerable target, read and become familiar with sensitive information, and determine the best time to execute a malicious act. Insider acts could include, for example, tampering with safety equipment to prepare for an attempt or act of sabotage, photocopying sensitive information, photographing security systems, mapping ingress and egress routes, and understanding shift rotations and staffing. An insider could also create site or workplace conditions, other than radiological sabotage, to thwart the licensee's ability to respond to a safety or security event. Delaying or preventing site personnel access to such structures, systems and components could adversely affect the safe operation of the plant or diminish security response force effectiveness, or both, and therefore adversely affect public health and

safety and the common defense and security. Therefore, a comprehensive IMP is one that is designed to address a broad context of trustworthiness and reliability issues to prevent or minimize the potential for malicious actions by an insider. Licensees should consider and be observant of subtle changes in an individual's behavior or actions over time and use appropriate IMP elements (e.g., the behavioral observation program) to assess not only the individual's trustworthiness and reliability but to gain insights into his or her character and reputation (10 CFR 73.56(d)(6)) to aid in the licensee reviewing official's access authorization assessment and perhaps prevent the individual from executing subversive acts.

As described in 10 CFR 73.56(a), a licensee is required to establish, implement, and maintain an access authorization program, as a part of its physical protection program, for granting unescorted access to the protected and vital areas of a nuclear power plant. The general performance objective of the access authorization program is to provide high assurance that individuals granted unescorted access are trustworthy and reliable and do not constitute an unreasonable risk to public health and safety, including the potential to commit radiological sabotage.

As described in 10 CFR 73.56(c) through (f), licensees implement measures to ensure that a person does not possess behavioral characteristics that may indicate current or future propensity to be untrustworthy and unreliable. These measures will typically provide information that also supports the licensee's IMP.

As described in 10 CFR 73.56(f), (g), (i), and (j), in conjunction with the IMP requirements, licensees must ensure, following their initial determination of unescorted access, continued trustworthiness and reliability of those individuals with unescorted access to a facility, as well as maximize opportunities to identify insider activity. The paragraphs below describe possible methods for licensees to ensure continued trustworthiness and reliability.

Licensees should analyze their programs and industry or other insider-related events by considering, but not limited to, sources such as NRC information notices (INs), regulatory information summaries, or other official accounts of events as well as information shared within the industry to ensure that their policies, actions, and measures provide a level of protection that meets the IMP requirements.

The licensee's, or applicant's, reviewing official may grant, deny, suspend, withhold, revoke, or terminate unescorted access or unescorted access authorization; determine what level of access, if any, an individual will have; and make all final decisions on unescorted access to its facilities in accordance with 10 CFR 73.56. These requirements are implemented with those of 10 CFR 73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to safeguards information," and the escorted access requirements mandated in 10 CFR 73.55(g)(7).

Licensees should not allow an individual who demonstrates questionable behavior (as discussed in 10 CFR Part 26 and 10 CFR 73.56) to retain unescorted access because doing so degrades the licensee's ability to prevent adverse acts. The effect of such failure improperly places the burden of insider mitigation solely on the physical protection elements (e.g., physical controls, contraband searches, and security patrols) of the licensee's physical protection program.

Licensees must implement the required elements of their cyber security plans as they address the requirements in 10 CFR 73.54, 10 CFR 73.55(b)(9), and 10 CFR Part 26, to provide high assurance that a person with access to digital computer and communications systems and networks from outside the protected area will not pose a significant threat to the safety and security of a nuclear power plant. Licensees may have difficulty identifying the cause of an incident, particularly for a cyber-related incident.

Mitigation of opportunities for insider tampering is particularly important because an insider may know how to manipulate various systems in ways that are difficult to detect. Any acts of wrongdoing or tampering are particularly serious matters because of the potential adverse impact on nuclear power plant safety and security that could adversely affect the protection of public health and safety and the common defense and security.

It is important to recognize that the IMP alone does not address all cyber threats and attack vectors. As a result, the IMP alone does not take the place of other cybersecurity requirements and controls used to mitigate outside cyberattack vectors and pathways that pose a threat to equipment.

There is a broad spectrum of motivations related to possible insider threats that range from the premeditated actions of an individual acting alone as a single source of origin (e.g., disgruntled employee) to events that might be sufficient to motivate someone to act (e.g., extortion). The highly unpredictable nature of the insider threat requires a comprehensive approach to address both the intent and capability of the potential insider.

All individuals who are subject to 10 CFR 73.55 should be aware of and trained to report behaviors that would typically lead to or manifest themselves in behaviors or activities of a potential insider, and licensees should implement their IMP programs in a manner that ensures the coordination that provides the defense in depth necessary to mitigate the insider threat. For example, access authorization personnel should work closely with employee assistance program (EAP) personnel, an element of the FFD program described in 10 CFR Part 26, to ensure that individuals demonstrating any potential to harm themselves or others are reported to appropriate security personnel for evaluation as a potential insider threat, without creating the perception that seeking help through the EAP will result in adverse action. In addition, licensee personnel should be able to recognize and report behaviors adverse to the safe operation and security of the facility, including unusual interest in security practices, security procedures, or involvement in security or operational activities outside an employee's normal work scope.

2. Applicability

The IMP is applicable to any individual granted or maintaining unescorted access to a protected or vital area. It is designed to provide defense in depth to minimize the potential for an insider to cause significant core damage or spent fuel sabotage. At a minimum, to mitigate the potential for an insider to be successful, and as directed by EA-03-086, dated April 29, 2003, Attachment 2 (NS108308) (Ref. 14), an IMP must consist of the following elements for all personnel with unescorted access to the protected and vital areas of a facility, or those who have been certified for unescorted access authorization: (1) a security determination (clearance or access authorization), (2) initial and random substance abuse testing, (3) initial and periodic medical assessment, to include psychological evaluations, (4) review by the immediate supervisor at least annually, and (5) periodic reinvestigation of the security determination (clearance, access authorization, or both). RG 5.66 contains additional guidance. The requirements in 10 CFR 73.55 remain applicable even after a licensee submits the certifications required by 10 CFR 50.82, "Termination of license."

General Applicability

The IMP applies to all persons who are granted or retain unescorted access authorization to a protected or vital area. Licensees should evaluate whether to include personnel assisting with unescorted access determinations, such as FFD program personnel and certain persons who have duties and responsibilities in the Emergency Operations Facility, as described in Section C.2.2.3 of this RG. Insiders may occupy any position within a licensee's organization, and the IMP applies to all personnel that are in

an unescorted access status or are certified for unescorted access authorization. Persons in the critical group are considered to present a greater risk as an insider threat because of their knowledge of the plant, access to vital plant equipment, access to drug and alcohol records, and authorization determinations, or because they are in possession of weapons inside the protected area of a licensed facility.

2.1 The Critical Group

Although the NRC's regulations do not use the term "critical group," this RG uses the term to include, at a minimum, those individuals identified in 10 CFR 73.56(b) and who provide services or perform one or more job functions that are critical to the safe and secure operation of the licensee's facility. The glossary to this RG further defines the term "critical group."

As described in 10 CFR 73.56(i)(1)(v)(B), the trustworthiness and reliability determination for any individual in the critical group must be reestablished within 3 years of the date on which that determination was last made, or more frequently, based on factors determined by the licensee or applicant. At a minimum, as described in 10 CFR 73.56(i)(1)(v)(B), the current determination shall be based on a criminal history update and credit history reinvestigation within 3 years of the date on which these elements were last completed and a psychological reassessment within 5 years of the date the last psychological assessment was completed.

Note: To further clarify 10 CFR 73.56(i)(1)(v)(B)(4), the term "information technology (IT) personnel" has been further defined in the glossary and is consistent with Security Frequently Asked Question (SFAQ) 10-05, "IT Functions for the Critical Group," dated April 4, 2010 (Ref. 15).

2.2 Other Personnel for Consideration

Licensees may determine that it is desirable to place additional personnel, beyond those required by regulation, under the IMP to provide a higher degree of assurance in the trustworthiness and reliability of those individuals who perform job duties that are critical to nuclear power facility safety and security. The decision to include additional personnel should be based on the licensee's IMP performance objectives associated with mitigating active insider, active violent insider, and passive insider threats.

2.2.1 For example, licensees may wish to include those persons who have an "L" or "Q" security clearance under 10 CFR Part 11, "Criteria and Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material" (Ref. 16), or 10 CFR Part 25, "Access Authorization" (Ref. 17), respectively, within the scope of the IMP even if they do not have unescorted access or unescorted access authorization because they may possess information that could aid an insider.

2.2.2 The IMP may apply to those persons necessary for the effective implementation of the drug and alcohol testing provisions as described in this guide. The IMP may include personnel who are involved in the day-to-day operations of the FFD program, as defined by the procedures of the licensees and other entities, and whose duties require them to have the following types of access or perform the following activities:

a. the FFD coordinator/supervisor responsible for the implementation of the drug and alcohol testing program on site,

b. persons on the FFD program staff involved in selecting (e.g., determining, reading, or implementing the random test list and determining when random testing will be

conducted) or notifying the individuals (or the individuals' supervisor or manager) for testing,

c. persons involved in the collection (e.g., collectors if they are licensee employees) or onsite testing of alcohol or urine specimens,

d. persons, including the Medical Review Officer, site nurse, or medical practitioner, when on site, who do the following:

(1) review or act on EAP findings that represent a concern about a licensee or other entity's trustworthiness or reliability determination for an individual (e.g., 10 CFR 26.35(c)(2)(i)), and

(2) can link test results with the individual who was tested before an FFD policy violation determination is made; and

e. persons who make authorization decisions under 10 CFR Part 26, Subpart C, "Granting and Maintaining Authorization."

2.2.3 The licensee may consider whether to apply the IMP to persons designated to physically report to the Emergency Operations Facility and those persons who may have access to sensitive (e.g., security- or safety-related) information.

3. Elements of an Insider Mitigation Program

3.1 Fitness for Duty Elements

3.1.1 Drug and Alcohol Testing Provisions

3.1.1.1 Under 10 CFR 73.55(b)(9)(ii)(B), nuclear power reactor licensees are required to include elements of the FFD program described in 10 CFR Part 26 in their IMP.

a. Licensees of power reactors that are licensed to operate under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," must implement all FFD program elements described in 10 CFR Part 26.

b. Those 10 CFR Part 50 licensees that have submitted the certifications required by 10 CFR 50.82(a) may implement all FFD program elements described in 10 CFR Part 26. Another acceptable approach would be to implement the 10 CFR Part 26 elements described below.

3.1.1.2 The drug and alcohol testing provisions considered adequate for the IMP are those that provide reasonable assurance that the drug and alcohol testing program is effectively and consistently implemented and that individuals meet the following criteria:

a. trustworthy and reliable as demonstrated by the avoidance of substance abuse and

b. not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause that in any way adversely affects their ability to perform their duties safely and competently.

3.1.1.3 Drug and alcohol testing provisions may be implemented through a licensee's policy and procedures.

3.1.1.4 RG 5.66 describes additional guidance on authorization determinations based on drug and alcohol test results.

3.1.1.5 Licensees should consider the potential insider threat when making FFD determinations under 10 CFR 26.189(c)(2). For example, licensee or other entity management personnel should implement the required actions to ensure any potential limiting condition does not represent a threat to workplace or public health and safety.

3.1.2 Behavioral Observation, 10 CFR 26.33

Licensees and other affected entities must ensure that the individuals who are subject to 10 CFR Part 26, Subpart B, "Program Elements," are also subject to a behavioral observation program that meets the requirements specified in 10 CFR 26.33, "Behavioral observation," and 10 CFR 73.56(f). Although behavioral observation includes the early identification of many other behaviors that may pose a risk to a nuclear power plant or spent fuel pool, it is performed by individuals trained under 10 CFR 26.29, "Training," to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcohol; or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security. Further, individuals should be trained in recognizing and reporting behaviors as required in 10 CFR 73.56(f), which may be considered adverse to the safe operation and security of the licensee facility.

Licensees and other affected entities shall ensure that the individuals who are subject to 10 CFR Part 26, Subpart B are subject to behavioral observation. Behavioral observation is performed by individuals trained under 10 CFR 26.29 to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcoholic beverages, or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security. The requirements of 10 CFR 26.33 and 10 CFR 73.56(f) are captured in RG 5.66. Implementing these requirements helps provide high assurance of an effective behavioral observation program at operating and decommissioning power reactors.

RG 5.66 contains guidance to support the behavioral observation requirements specified in 10 CFR 26.33 and 10 CFR 73.56(f). Licensees may use this RG for guidance in providing a combined FFD and access authorization behavioral observation program. Implementing these requirements helps provide high assurance of an effective IMP. Section C.4 of this RG provides additional guidance.

3.1.3 Employee Assistance Program, 10 CFR 26.35

Licensees and other affected entities shall maintain an EAP to strengthen the FFD program by offering confidential assessment, short-term counseling, referral services, and treatment monitoring to individuals who have problems that could adversely affect the individual's ability to perform their duties safely and competently. As applied to the trustworthiness and reliability of persons subject to an IMP, the EAP enables a person to self-refer and allows for early intervention when problems arise. Further, EAP personnel have an opportunity to determine or identify when an individual may pose or has posed an immediate or latent hazard to him or herself or to others. When such a situation arises, EAP personnel can inform FFD program management.

These situations include, but are not limited to, substantive reasons to believe that the individual (1) is likely to cause self-harm or harm to others, (2) has been impaired from using drugs or alcohol while in a work status and has a continuing substance abuse disorder, or, (3) has ever been engaged in any acts that would be reportable under those requirements mentioned in 10 CFR 26.719(b)(1) through (b)(3) and 10 CFR Part 73, Appendix G, "Reportable Safeguards Events."

3.1.4 Reporting of Fitness for Duty Program Performance Information

The reporting provisions for FFD programs appear in 10 CFR 26.717, "Fitness-for-duty program performance data," and 10 CFR 26.719, "Reporting requirements." Reporting enables effective regulatory oversight of conditions adverse to safety or security. Trending of this performance information also informs licensee assessments of program implementation and the conduct of NRC inspections to provide assurance that programmatic implementation meets regulatory requirements.

3.1.5 Elements Not Associated with Trustworthiness and Reliability

The NRC acknowledges that some drug and alcohol testing provisions are not necessary to ascertain whether an individual is trustworthy and reliable. Table 1 shows these provisions.

Table 1. Drug and Alcohol Testing Provisions Not Associated with Trustworthiness and Reliability

	Drug and Alcohol Provisions	Reference Requirement
a	Performance Objectives	10 CFR 26.23(e)
b	Audits and Corrective Actions	10 CFR 26.41(c)(1) and (2) (Note 1); and 10 CFR 26.41(e) (Note 2)
c	Collection Sites, Preparation, and Testing	10 CFR 26.85, 26.87, 26.89, 26.91, 26.93, 26.95, 26.97, 26.99, 26.101, 26.103, 26.105, 26.107, 26.109, 26.111, 26.113, 26.115, 26.117, and 26.119 (Note 3)
d	Quality Assurance and Quality Control	10 CFR 26.167 (Note 4)
e	Blind Performance Testing	10 CFR 26.168 (Note 4)
f	FFD Program Performance Data	10 CFR 26.717(b)(9) (Note 5)
g	Reporting Requirements	10 CFR 26.719(c) (Note 6)

Note 1: Auditing of a blind performance specimen provider and the primary and secondary U.S. Department of Health and Human Services-certified laboratories is not an element of 10 CFR Part 26 necessary to determine the trustworthiness and reliability of individuals subject to the IMP; however, assessing performance provides assurance that specimen test results are accurate. As a result, the licensee should consider implementing an audit program in accordance with 10 CFR Part 26.

In lieu of the above guidance, if a decommissioning licensee elects not to audit both its laboratories and the blind performance test sample (BPTS) supplier on an annual basis, then the licensee should annually verify the following:

- that the laboratories process specimens from, and the BPTS supplier provides specimens to, at least one other NRC licensee in accordance with 10 CFR Part 26

and ensure that these programs are audited subject to the audit requirement under 10 CFR 26.41, "Audits and corrective action;"

- that at least one other operating reactor's audit report is shared with the decommissioning licensee; and

- that significant performance issues have not been identified, noting that a significant performance issue is one identified by any licensee using the laboratory or BPTS supplier in which performance resulted in a condition adverse to 10 CFR Part 26 program effectiveness (e.g., procedure issues, failure to conduct limit of detection testing, blind or quality control specimen failures (see Note 4)) and adequate corrective actions were not implemented by the laboratory or blind performance test supplier to prevent recurrence.

Audits can be conducted with those performed by other NRC-licensed facilities or led by the NEI on behalf of a facility or multiple facilities. This audit provision is also based on the relatively few specimens expected to be provided by and to a licensee that has submitted its 10 CFR 50.82 certifications because access authorization will be limited to fewer persons (i.e., fewer persons subject to testing) when compared to the total number of federally mandated tests being processed by other users.

Note 2: Audits should be conducted by persons who are knowledgeable of the area being audited and should be independent of the program area being audited. If independence cannot be achieved, the audit should be supplemented by a co-reviewer that provides independence with reasonable knowledgeable of the area being reviewed. The manager, supervisor, and technician responsible for FFD program implementation, including drug and alcohol testing, may audit the offsite collection facility, laboratory, and blind sample supplier.

Note 3: The use of a collection facility meeting the requirements of 10 CFR 26.87, "Collection sites," provides reasonable assurance that specimen collections will be conducted consistently, accurately, and effectively; however, the use of a local hospital or other facility (e.g., occupational health center) to collect and process specimens provides equivalent assurance that the 10 CFR 26.87 provisions are implemented. Further, the use of an offsite collection facility enables the decommissioning of the NRC-licensed facility. All personnel should use a collection facility meeting the requirements of 10 CFR 26.87 or 49 CFR Part 40, "Procedures for Transportation Workplace Drug and Alcohol Testing Programs" (Ref. 18), to provide consistency in collection services, except if the licensee implements a short-duration transition period (e.g., less than 90 days) when shifting from an onsite to an offsite collection facility.

Note 4: The quality assurance and quality control (QA/QC) and blind performance specimen testing provisions in 10 CFR 26.167, "Quality assurance and quality control," and 10 CFR 26.168, "Blind performance testing," provide assurance that laboratories and BPTS suppliers are performing to acceptable standards. As a result, the licensee should consider using the requirements specified in 10 CFR 26.167 and 10 CFR 26.168.

In lieu of following 10 CFR 26.167 and 10 CFR 26.168, the licensee could annually verify that (1) both laboratories process QA/QC and blind samples from at least one other NRC licensee in accordance with 10 CFR Part 26, and (2) the BPTS supplier provides specimens to at least one other NRC licensee. The licensee should also verify that significant laboratory and BPTS supplier performance issues have not been identified by the other NRC

licensee(s) using the laboratories and BPTS supplier. A significant issue is one that resulted in a condition adverse to 10 CFR Part 26 program effectiveness (e.g., a procedure issue; failure to confirm; a 10 CFR 26.719 reportable event) and the laboratory or BPTS supplier did not implement adequate corrective actions to prevent recurrence. Laboratory and BPTS supplier performance could also be ascertained from a review of operating experience gathered by other NRC-licensed facilities or the NEI. This QA/QC BPTS provision is also based on the relatively few specimens expected to be provided by a licensee that has submitted its 10 CFR 50.82 certifications because access authorization will be limited to fewer persons (i.e., fewer persons subject to testing) when compared to the total number of federally mandated QA/QC and blind sample tests being processed by other NRC licensees using the site primary and backup U.S. Department of Health and Human Services-certified laboratories and BPTS supplier.

Note 5: The provisions of 10 CFR Part 26, Subpart I, "Managing Fatigue," are not elements of 10 CFR Part 26 necessary to determine the trustworthiness and reliability of individuals subject to the IMP; therefore, this provision is not applicable. However, fatigue management helps provide reasonable assurance that individuals can safely and competently perform assigned duties and responsibilities.

Note 6: The IMP does not need to include the reporting requirements of 10 CFR 26.719(c)(1) – (3), except for the Medical Review Officer and random testing error provisions, unless the licensee decides to conduct QA/QC and BPTS performance testing and discovers reportable errors associated with the testing of their specimens.

3.2 Access Authorization Program Elements

3.2.1 Initial Security Determination

Initial security measures for completing background investigations and other programmatic elements required by the NRC, through the implementation of the requirements of 10 CFR 73.56 and 10 CFR 73.57 and consistent with guidance contained in RG 5.66, provide high assurance that persons initially certified for unescorted access authorization or granted unescorted access are trustworthy and reliable and do not present a risk to public health and safety or the common defense and security.

3.2.2 Psychological Assessments, including Medical Evaluations—Initial and Periodic

3.2.2.1 As required under 10 CFR 73.56(e), the psychological assessment must be designed to evaluate the possible adverse impact of any noted psychological characteristics on the individual's trustworthiness and reliability. Under 10 CFR 73.56(e)(1), the psychological assessment must be conducted by a licensed psychologist or psychiatrist with the appropriate training and experience.

a. Before any psychological or medical assessment, the appropriate practitioner should review a current position description for the person being interviewed and the most recently completed supervisory review, if applicable, for information that could assist the appropriate practitioner in his or her assessment.

b. Initial psychological assessments should ensure that any testing mechanism applied, in whole or in part, to a psychological determination of suitability for unescorted access includes the opportunity to detect the need for a medical evaluation.

3.2.2.2 As stated in 10 CFR 73.56(e)(3) and (e)(4), the psychological assessment must include the following:

a. the administration and interpretation of a standardized, objective, professionally accepted psychological test that provides information to identify indications of disturbances in personality or psychopathology that may have adverse implications for an individual's trustworthiness and reliability, and

b. a clinical interview if the individual receives scores on the psychological test that identify indications of disturbances in personality or psychopathology that may have implications for an individual's trustworthiness and reliability; or if the individual is a member of the population that performs one or more job functions that are critical to the safe and secure operation of the licensee's facility.

3.2.2.3 The initial and periodic assessment should consider the psychopathology of the interviewee. Psychiatrists or clinical psychologists with the appropriate clinical training and experience should consider applying procedures of evaluation assessment and diagnosis derived from scientific research.

3.2.2.4 The administration of a psychological assessment may trigger a medical evaluation to determine the presence of any mental or physical condition that may cause a concern about the individual's trustworthiness and reliability. Medical evaluations triggered by a psychological recommendation should include a review of the individual's prescribed medications to ensure that these medications do not impair the person's ability to safely and competently perform assigned duties or adversely affect his or her trustworthiness and reliability. Individuals identified as candidates for further medical review should be referred to a physician who may be qualified as the Medical Review Officer, for further evaluation (see 10 CFR 26.189, "Determination of fitness"). Medical personnel should evaluate possible medical conditions, including those that may result from the use of illegal drugs; the abuse of prescribed or over the counter medications; or the excessive, habitual use of alcohol, in accordance with the provisions of 10 CFR Part 26.

3.2.2.5 During psychological reassessments, if the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the FFD or trustworthiness and reliability of any individual who currently has unescorted access or unescorted access authorization, the psychologist or psychiatrist shall, in accordance with 10 CFR 73.56(e)(6), inform (1) the reviewing official of the discovery within 24 hours of the discovery, and (2) the medical personnel designated in the site implementing procedures who shall ensure that an appropriate evaluation of the possible medical condition is conducted consistent with 10 CFR Part 26. The results of the evaluation and a recommendation shall be provided to the licensee's or applicant's reviewing official. The interviewing licensed psychologist or psychiatrist should incorporate the most recent supervisory review or interview, as applicable, as one measure of the assessment.

3.2.2.6 As stated in 10 CFR 73.56(i)(1)(v)(B), the psychological assessment must be conducted within 5 years of the date on which the last psychological assessment was completed. As part of complying with 10 CFR 73.56(i)(1)(v)(B), licensees should consider conducting interviews in a semi-structured manner. These interviews should include the recognition of medical conditions that could result in impaired judgments or could adversely impact the FFD or trustworthiness and reliability of those individuals who currently have unescorted access or unescorted access authorization status. While other types of interviews are permitted, a face-to-face interview

conducted by an interviewer trained to look for precursors of insider behavior is preferable for identifying persons with potentially undesirable behavioral issues.

3.2.2.7 As stated in 10 CFR 73.56(i)(1)(vi), failure to complete the psychological reassessment within the time frame specified under 10 CFR 73.56(i)(1)(v) is one basis for the licensee or applicant to administratively withdraw the individual's unescorted access or unescorted access authorization until the reassessment has been completed.

3.2.3 Annual Review by Immediate Supervisor

A review conducted by the assigned supervisor has value as an integral part of the behavioral observation program required by 10 CFR 73.56(i)(1)(iv). This review creates a platform for interaction between the supervisor and the employee to the extent that the supervisor could become aware of any condition that may cause the employee to act or behave in an unconventional manner. In addition, the supervisory review provides an opportunity for the supervisor to consider whether any circumstances may indicate the need to refer the employee for additional medical or psychological review.

The annual supervisory review or interview should incorporate the consideration of any self-reporting as required in 10 CFR 73.56(g).

3.2.3.1 In some cases, the supervisor may not have frequent enough personal interaction with the individual throughout the review period to develop an informed and reasonable opinion about the individual's behavior, trustworthiness, and reliability. When this unusual condition occurs, the interview may consist of face-to-face contact and the gathering of information from personnel who have had frequent interaction with the individual, combined with other documented methods of gathering information, to ensure the supervisor can attest to the individual's continued trustworthiness and reliability.

3.2.3.2 In addition to the requirements noted above, a supervisory review may incorporate information developed over the covered period (i.e., annually) about the behavioral characteristics of the employee supervised. This information would typically include deviations from the behavioral norm that have been reported to the supervisor through the implementation of the behavioral observation program, as well as those deviations personally observed by the supervisor. This review serves two purposes. First, it can identify issues related to physical or mental impairment that fall under the general performance objectives of 10 CFR Part 26. Second, it can identify issues related to trustworthiness and reliability other than those related to physical or mental impairment.

3.2.4 Periodic Reinvestigation of Security Determination

3.2.4.1 All individuals maintaining unescorted access or unescorted access authorization must, at a minimum, meet the requirements of 10 CFR 73.56(i)(1)(i)(v)(A), (C), and (vi).

3.2.4.2 Under 10 CFR 73.56(i)(1)(v)(B)(1) – (5), members of the critical group must be reinvestigated within 3 years of the date on which the criminal history update and credit history reevaluation were last completed, or more frequently, based on job assignment as determined by the licensee or applicant. The requirements of this section apply to all individuals certified for unescorted access authorization or granted unescorted access who are members of the critical group. As required by 10 CFR 73.56(i)(1)(vi), individuals who have not satisfied reinvestigation requirements shall have unescorted access authorization or unescorted access administratively

withdrawn until reinvestigation has been completed. The individual may be reassigned to noncritical group positions until the required critical group reassessment can be completed. In addition, any individual not assigned to the critical group is reinvestigated within 5 years of the date on which the criminal history update and re-evaluation elements were last completed.

The reinvestigation includes the following:

a. Licensees shall review criminal history records obtained under 10 CFR 73.56(d)(7) and 10 CFR 73.57, or as the Commission may require, or as Federal statutes may direct. Licensees should compare data returned from the criminal history records check with the access authorization records of the person named in the record to ensure that the person has complied with the self-reporting requirements in 10 CFR 73.56(g). Licensees should prioritize fingerprint requests to ensure there are no unanticipated staffing issues.

b. Licensees shall obtain a full credit history and review the history for the period provided as required by 10 CFR 73.56(d)(5). The individual should complete new consent to screen and Fair Credit Reporting Act disclosure and authorization statement forms before initiating this reinvestigation.

c. Licensees shall review any potentially disqualifying information during a reinvestigation against the licensee's program policies and procedures and act as appropriate.

d. The start of the interval for the next reinvestigation should be the date the reviewing official completed a concurrent review of both the credit history and criminal history information. To provide for reasonable consistency of the timeframe under review, in accordance with 10 CFR 73.56(i)(1)(v)(C), the reviewing official should ensure that the receipt of the credit history and the criminal history information are within 30 days of each other.

3.2.5 Access to Vital Areas

As required by 10 CFR 73.56(j), a licensee shall establish, implement, and maintain a list of individuals who are authorized to have unescorted access to specific nuclear power plant vital areas during nonemergency conditions. The rule requires that access authorization lists be updated and reapproved no less frequently than every 31 days. The list must include only those individuals who have a continued need for unescorted access to those specific vital areas to perform their duties and responsibilities. The list must be approved by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each vital area.

This requirement is to ensure that access authorization is only provided to those individuals who have a need to enter the vital area. This control helps mitigate insider threats by reducing the number of individuals having unescorted vital area access and by limiting vital area access to those personnel who specifically require access to vital areas in order to perform their duties, not just a possibility of needing access sometime in the future. Licensees must ensure that persons who are directing the work activity of persons with unescorted access are responsible for fulfilling behavioral observation requirements of persons with unescorted access and recertifying the continued need for vital area unescorted access no less frequently than every 31 days. The NRC recognizes that a single licensee manager or supervisor would not have oversight and control of every person with unescorted access to any or all of the licensee's vital areas.

In determining continued need, licensees should consider event response, weekend or holiday emergencies, or other "off hours" operational or emergency responses. The licensee may determine that some individuals need to remain on the list for emergency response purposes even though the frequency of entry into a particular vital area is limited. Personnel who fall into this emergency response category must be evaluated for continued need for access during the 31-day review by a cognizant licensee or applicant manager or supervisor who would be responsible for directing the work activities of the individual while that individual is present at the licensee or applicant site.

3.3 Cybersecurity Elements

Pursuant to 10 CFR 73.55(b)(9)(ii)(C), a licensee's IMP must contain elements from the cybersecurity program described in 10 CFR 73.54. As required by 10 CFR 73.54(a), a licensee's cybersecurity program must provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat as described in 10 CFR 73.1. RG 5.71 provides guidance on the implementation of the NRC's cybersecurity requirements and provides a framework for the identification of those digital assets that must be protected from cyberattacks.

One means of complying with the requirement to include cybersecurity elements in the IMP is to ensure that the applicable cybersecurity controls identified in RG 5.71 are applied to the digital computer and communication systems and networks routinely used by members of the critical group, particularly IT personnel. The glossary of this RG defines "critical group" and "information technology (IT) personnel" as the terms are used in 10 CFR 73.56(i)(1)(v)(B). These definitions are consistent with those given in SFAQ 10-05. By establishing, maintaining, and successfully integrating these security controls into a site-specific cybersecurity program and referencing these controls in the IMP, the licensee can provide assurance of an effective IMP.

3.4 Physical Protection Plan Elements

3.4.1 Licensees should have procedures available for operator response to events involving deliberate acts directed against plant equipment. The NRC has issued two information notices (INs) to address conditions that could be potential insider threats.

a. On May 4, 1983, the NRC published IN 83-27, "Operational Response to Events Concerning Deliberate Acts Directed Against Plant Equipment" (Ref. 19), which provides licensees with information needed to formulate programmatic activities that licensees could consider in preparing for and responding to insider-directed behaviors. IN 83-27 describes events in which licensees were not prepared to assess situations and take necessary steps to ensure the operability of systems important to safety or make informed decisions concerning continued operation. The IN states, in part, that guidelines or procedures prepared by the licensee outlining a process for follow-up of both deliberate and inadvertent acts with respect to plant operation should be available.

b. On December 27, 1996, the NRC published IN 96-71, "Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief" (Ref. 20). IN 96-71 provides additional information for licensees to consider beyond the information in IN 83-27 in the form of examples of known and unexplained conditions that were inconsistent with routine operations. It also reminds licensees that events like those described in the IN must be reported to the NRC Operations Center within 1 hour of discovery, as described in Appendix G to 10 CFR Part 73.

3.4.2 In considering program elements needed to mitigate threats from the active insider and active violent insider, licensees should develop a program that will do the following:

a. Ensure that licensed operators are properly trained to recognize indications of tampering, which includes pre-positioning of equipment; to report such conditions promptly; and to compensate for degraded conditions as appropriate.

b. Ensure that armed security officers are properly trained to recognize obvious indications of tampering as required in 10 CFR 73.55(i)(5)(vii), and 10 CFR Part 73, Appendix B, "General Criteria for Security Personnel," Section VI.D.1(b)(1).

c. Ensure that personnel who receive plant access training are taught to recognize behaviors or conditions adverse to safe operations and security of the facility.

d. Develop procedures and training requirements to react effectively to conditions related to actual or suspected tampering as required in 10 CFR 73.55(i)(5)(vii).

e. Ensure that indications of tampering are included in the corrective action program as required in 10 CFR 73.55(b)(10).

f. Conduct random patrols of target set equipment or elements as required in 10 CFR 73.55(i)(5)(vi).

3.4.3 The program should identify and provide training to address target set equipment or elements that could be disabled locally, would not be observable from remote indications (e.g., the control room), and are factored into checks conducted during operator rounds on each shift. In developing program guidance, licensees should consider the operational importance of each target set element and its relative susceptibility to tampering.

a. While the above physical protection measures relate to target set equipment or elements, licensees should remain aware that tampering with nontarget set equipment or support systems, such as safety, security, and important to safety or emergency preparedness equipment, can adversely affect the ability to respond to events and comply with established regulations.

b. Licensees should train operations personnel to be sensitive to abnormalities that could be the result of tampering and to respond to such indications promptly. During routine tours, operations personnel should be sensitive to changes in configurations that might indicate possible tampering. Licensees should review, determine, and train operations personnel for target sets and target set equipment that may be disabled locally without any recognition by control room personnel that the equipment had been disabled before operation.

c. As described in 10 CFR 73.55(i)(5)(vii), licensees shall train security personnel to recognize and respond to obvious indications of tampering. In accordance with 10 CFR 73.55(i)(5)(vi), licensees are required to provide random patrols of all accessible areas containing target set equipment. These patrols should be conducted by an armed security officer and should include all target set equipment or elements, except when precluded by immediate personnel safety concerns, operational abnormalities, or

restrictions, consistent with guidelines to keep radiation dose rates as low as reasonably achievable.

d. As described in 10 CFR 73.55(i)(5)(iii), upon detection of tampering or other threats, the licensee shall respond in accordance with the security plans and implementing procedures. Any suspected tampering event should be entered into the licensee's corrective action program and reported as required by 10 CFR 73.71, "Reporting of safeguards events."

e. Licensees should implement an armed patrol program applying special consideration to target set equipment. These patrols should also periodically assess the integrity of the barriers protecting and controlling access to target set equipment. RG 5.76 describes approaches acceptable to the NRC for meeting these requirements.

Licensees may substitute surveillance and tamper detection mechanisms for armed patrols if these mechanisms can notify the response force in a timely manner. A sophisticated tamper indication device could be installed (e.g., three-dimensional video motion detection) and a camera assessment system used for rapid notification. Section 4.6.4, "Insider Mitigation," and Section 5, "Security System Technology," of SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," issued September 2007 (Ref. 21), outlines additional guidance for these types of measures and is acceptable for use alone or in conjunction with NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide," issued April 2013 (Ref. 22). Armed patrols and surveillance mechanisms should provide for notification of at least two members of the response force. Licensees could also mitigate insider-directed behavior through the installation of proximity sensors. Section 4.4, "Proximity Sensors," of NUREG-1959 discusses proximity sensors in detail. Section 4.4.4, "Characteristics and Applications," of NUREG-1959 provides licensees with detailed information on implementation options.

f. Licensees should search personnel for contraband (weapons, explosives, or incendiary devices) in accordance with 10 CFR 73.55(h) before personnel enter the facility. This makes contraband searches an integral physical protection element of the IMP.

4. Behavioral Observation Training

4.1 A comprehensive and effective behavioral observation program will include a training program for recognizing and reporting behaviors as required in 10 CFR 73.56(f)(2) and 10 CFR 26.33, which may be considered adverse to the safe operation and security of the licensee facility.

4.2 Licensees should ensure that the behavioral observation program training includes recognition of and response to the following conditions or behavioral characteristics:

a. the recognition that changes in emotional state can happen quickly,

b. typical conditions that can trigger behavioral anomalies,

c. the need for early intervention after the recognition of changes in behavior that typically indicate changes in emotional state,

d. the recognition of uncharacteristic deviations in coworker interactions, uncharacteristic absences from work, uncharacteristic inattention to detail, or suspected alcohol or drug abuse,

e. individual(s) seeking information about the security of the facility not provided through normal means (e.g., training programs), including unusual interest in, or predisposition toward, security,

f. individual(s) eliciting information on operational activities outside the scope of normal work assignments (e.g., questioning of other persons at a level beyond mere curiosity about facets of a facility, or the purpose of a structure, its operations, security procedures, or other aspects) in a manner that would arouse suspicions in a reasonable person,

g. individual(s) disappearing from a work assignment without adequate explanation or frequent or unexplained absence(s) from work assignments,

h. individual(s) giving an unsatisfactory response when questioned about work activities (e.g., unusual, or inadequate response when confronted about being in a plant or office location outside of the worker's usual place of work),

i. individual(s) voicing actual or potentially threatening views or opinions that could be threatening to a nuclear facility,

j. individual(s) in any plant area where they may not belong (e.g., an individual in an area outside of his or her usual scope of activities who cannot give an appropriate explanation for being in the location),

k. suspicious circumstances that cannot be explained through operational means (e.g., abnormalities that could be vandalism or tampering) such as the following:

   (1) misaligned breakers or valves,

   (2) cut wires or cables,

   (3) foreign objects in machinery, reservoirs, or tanks, or

   (4) inappropriate holes drilled, punched, or cut in pipes, tubes, or hoses, or damage to a component such that its safety or security function is compromised,

l. behavior that appears to challenge the installation, or building integrity, or systems, including cybersecurity capabilities,

m. taking pictures or video of sensitive facilities without preauthorization, or recording personnel activities, buildings, or infrastructure in a manner that would arouse suspicions in a reasonable person (e.g., taking pictures or video of frequently used access points, personnel performing security functions (patrols, badge, or vehicle checking), and security-related equipment (perimeter fencing, security cameras, etc.)),

n. unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional interest such that a reasonable person would consider the activity suspicious (e.g., unusual observation through binoculars, questionable notetaking, attempting to measure distances, and other activities that have no apparent nexus to facility operations),

o. possession of unusual quantities of cell phones, pagers, or other devices, such that a reasonable person would suspect criminal activity,

p. unusual interest in site security concepts (weapons or tactics) or other unusual capabilities outside of ordinary work scope that would arouse suspicions in a reasonable person,

q. unusual interest in an organization's technology infrastructure,

r. communicating in a manner that implies any threat to damage a facility or infrastructure or commit acts of violence against a person or group of people, and

s. the need to report any of the above conditions to the employee's assigned supervisor or FFD program manager or access authorization program manager.

D. IMPLEMENTATION

The NRC staff may use this regulatory guide (RG) as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this RG to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests," (Ref. 23), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this RG in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

GLOSSARY

active insider	A person who, while in an unescorted access status and within the protected area, takes direct action to assist a design-basis threat (e.g., participates in planning, uses an authorized key card to open a controlled access door, creates an operational or security diversion, or impedes a response to the threat).
active violent insider	A person who, while in an unescorted access status and within the protected area, takes direct action to harm plant components, a member of the security force, or plant staff with the intent of preventing the operation of equipment or of preventing the person harmed from participating in protective or recovery strategies, or who takes action to engage and divert operations or security resources from normal protective or recovery strategies.
administrative withdrawal of unescorted access authorization/ unescorted access	A process to temporarily withhold unescorted access authorization/unescorted access from an individual while action is taken to complete or update an element of the unescorted access authorization requirements.
annual	Requirements specified as "annual" should be scheduled at a nominal 12 months. Performance may be conducted up to 3 months before to 3 months after the scheduled date. The next scheduled date is 12 months from the originally scheduled date, unless a midcycle activity is conducted to establish a new scheduled date.
applicant	Applicants for an operating license or holders of a combined construction permit and operating license (combined license) who choose to implement their access authorization programs, which were approved by the Commission in the applicants' physical security plan, before receiving their operating licenses or the Commission finding.
background investigation	Information from all background investigation elements to be collectively evaluated by the reviewing official pursuant to a determination of trustworthiness and reliability of an individual. Depending on the background investigation period, the elements may include any or all of the following: verification of true identity, employment verification with suitable inquiry (includes education in lieu of employment and military service as employment), a credit check, and character and reputation determination.
behavioral observation program	An awareness program that meets requirements of both the access authorization and FFD programs. Personnel are trained to report legal actions; possess certain knowledge and abilities related to drugs and alcohol and the recognition of behaviors adverse to the safe operation and security of the facility by observing the behavior of others in the workplace and detecting and reporting aberrant behavior or changes in behavior that might adversely impact an individual's trustworthiness or reliability; and undergo an annual supervisory review.
critical group	Any individual who performs job functions that are critical to the safe and secure operation of the licensee's facility. This individual includes anyone who has been granted unescorted access or certified with unescorted access authorization and performs one or more of the following job functions:

a. has extensive knowledge of facility defensive strategies or designs and/or implements the plant's defense strategies

b. can grant an individual unescorted access or to certify an individual unescorted access authorization

c. is assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices)

d. has the combination of electronic access and the administrative control (e.g., "system administrator rights") to alter one or more security controls associated with one or more critical digital assets (CDAs)

e. has extensive knowledge of the site-specific cyber defensive strategy "Extensive knowledge" is defined as having (1) knowledge of the cybersecurity controls in place for a CDA, or (2) knowledge of how the configuration of a CDA or the cybersecurity controls can be modified in a manner that could result in an adverse impact to safety or important-to-safety, security, or emergency preparedness (SSEP) functions.

Individuals performing the following functions should be included:

- site cybersecurity supervisors
- site cybersecurity manager
- site cybersecurity training manager
- corporate cybersecurity manager

"Administrative control" is defined as the electronic access and rights to independently change either the configuration of a CDA or the cybersecurity controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions.

Individuals performing the following functions should be included, as applicable:

- cybersecurity engineers and administrator,
- information technology personnel who are responsible for authorizing access to CDAs
- CDA system administrators
- personnel who can independently change the configuration of CDAs or can alter security controls

f. Licensed reactor operators.

g. Non–licensed operators. Non-licensed operators include those individuals responsible for the operation of plant systems and components, as directed by a reactor operator or senior reactor operator. Non-licensed operators also monitor plant instrumentation and equipment and principally perform their duties outside the control room.

fitness for duty (FFD) authorization

An element of unescorted access that identifies the status of an individual's required FFD elements, which are then evaluated by a reviewing official to determine the individual's trustworthiness, reliability, and FFD. These required elements for FFD authorization are consent, suitable inquiry (including education in lieu of employment and military service as employment), self-disclosure, pre-access drug and alcohol testing, and being subject to both a licensee-approved behavioral observation and random drug and alcohol testing program.

insider

A person who has been granted unescorted access or unescorted access authorization under the requirements of 10 CFR 73.56 or has the ability to access information systems that (1) connect to systems that connect to plant operating systems, or (2) contain sensitive information that may assist in an attempted act of sabotage.

information technology (IT) personnel

(1) Any individual who has the combination of electronic access AND the administrative control (e.g., "system administrator" rights) to alter one or more security controls associated with one or more CDAs should be in the critical group. A person with administrative control has the electronic access and rights to independently change either the configuration of a CDA or the cybersecurity controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions.

(2) Any individual with extensive knowledge of the site-specific cyber defensive strategy should also be in the critical group. "Extensive knowledge" is defined as having (a) knowledge of the cybersecurity controls in place for a CDA, or (b) knowledge of how the configuration of a CDA or the cybersecurity controls can be modified or leveraged in a manner that could result in an adverse impact to SSEP functions, or (c) knowledge of vulnerabilities of the site-specific cybersecurity defensive strategy.

Individuals performing the following functions should be included in the critical group:

- site cybersecurity supervisors
- site cybersecurity manager
- site cybersecurity training manager
- corporate cybersecurity manager
- cybersecurity engineers and administrators
- IT personnel who are responsible for authorizing access to CDAs
- CDA system administrators
- personnel who can independently change the configuration of CDAs or can alter cybersecurity controls

passive insider

A person who provides or attempts to provide safeguards information or other relevant information about a licensee's physical configurations, designs, strategies, or capabilities to any person who does not have a functional or operational need to know.

position description

A statement or description outlining the essential functions of a job and the potential exposures and hazards associated with those functions, or the environment in which the functions are executed.

reinvestigation	A periodic inquiry or assessment conducted to ensure that individuals continue to meet unescorted access authorization or unescorted access, or FFD program suitability requirements as defined in the most current NRC staff-endorsed version of NEI 03-01, "Nuclear Power Plant Access Authorization Program," which describes an approach that the NRC staff has found acceptable.
reviewing officials	Persons designated by the licensee or, if applicable, the contractor or vendor, to be responsible for reviewing and evaluating data collected about an individual, including potentially disqualifying information, to determine whether the individual may be certified for unescorted access authorization or granted unescorted access by a licensee.
semi-structured interview	An interview with an individual applying for unescorted access authorization or a person maintaining unescorted access authorization, conducted by a psychiatrist or a licensed psychologist with clinical experience as required by applicable State regulations. The interview contains questions determined appropriate by the interviewing psychiatrist or licensed psychologist, which vary the focus and content of the interview, depending on the written assessment, the observations of the interviewer, and the interviewee's responses to questions. The semi-structured interview may contain any other evaluative measure determined appropriate by the psychiatrist or licensed psychologist.
tampering	Deliberately damaging, disabling, or altering equipment necessary for safe shutdown or security equipment necessary for the protection of the facility in order to defeat their function or prevent them from operating.
target set	The minimum combination of equipment or operator actions that, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., non-incipient, nonlocalized fuel melting or core destruction) or a loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations.
unescorted access	Granted to an individual after satisfactorily completing all regulatory requirements for unescorted access authorization and FFD authorization and plant access training. The individual is subjected to a behavioral observation program, is placed in a random drug and alcohol testing program and is given the physical means to gain unescorted access to the protected area.
unescorted access authorization	Certification and status in the access authorization process that the individual satisfactorily completed all required elements as specified in Section 6 of NEI 03-01, Revision 3 (including these FFD authorization elements: consent, self-disclosure, suitability inquiry, and drug and alcohol testing elements defined in 10 CFR Part 26); is subject to a behavioral observation program; has training in the FFD knowledge and abilities; and was evaluated by a licensee reviewing official who then made a favorable determination of the individual's trustworthiness, reliability, and FFD.

REFERENCES [2]

1. *U.S. Code of Federal Regulations* (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter 1, Title 10, "Energy."

2. CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

3. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

4. CFR, "Fitness for Duty Programs," Part 26, Chapter 1, Title 10, "Energy."

5. U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 5.66, "Access Authorization Program for Nuclear Power Plants," Washington, DC.

6. Nuclear Energy Institute, NEI 03-01, Revision 3, "Nuclear Power Plant Access Authorization Program," Washington, DC.

7. NRC, RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements" (SGI), Washington, DC.

8. NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

9. NRC, RG 5.76, "Physical Protection Programs at Nuclear Power Reactors" (SGI), Washington, DC.

10. NRC, NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," Revision 1, Washington, DC, September 2017. (ML17250A867)

11. NRC, "Nuclear Regulatory Commission International Policy Statement," *Federal Register*, Vol. 79, No. 132, pp. 39415–39418, Washington, DC, July 10, 2014.

12. NRC, Management Directive 6.6, "Regulatory Guides," Washington, DC, May 2, 2016. (ML18073A170)

---

2 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at https://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at https://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at (301) 415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov. Documents that are withheld from the public can be requested by those individuals who have established a "need-to-know" and possess access permission to Official Use Only—Security Related Information (OUO-SRI) or safeguards information (SGI) (or security clearance for classified documents).

13. International Atomic Energy Agency, IAEA Nuclear Security Series No. 8-G, "Preventive and Protective Measures against Insider Threats," Revision 1, Vienna, Austria, 2020.[3]

14. EA-03-086, April 29, 2003, Attachment 2 (SGI) (NS108308).

15. Security Frequently Asked Questions 10-05, "IT Functions for the Critical Group," April 4, 2010. (ML102100070)

16. CFR, "Criteria and Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material," Part 11, Chapter 1, Title 10, "Energy."

17. CFR, "Access Authorization," Part 25, Chapter 1, Title 10, "Energy."

18. CFR, "Procedures for Transportation Workplace Drug and Alcohol Testing Programs," Part 40, Chapter 1, Title 10, "Energy."

19. NRC, Information Notice 83-27, "Operational Response to Events Concerning Deliberate Acts Directed against Plant Equipment," Washington, DC, May 4, 1983. (ML082831453)

20. NRC, Information Notice 96-71, "Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief," Washington, DC, December 27, 1996. (ML031050461)

21. Sandia National Laboratories, SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," Albuquerque, NM, September 2007.[4] (ML072620172)

22. NRC, NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide," Washington, DC, April 2013. (ML13122A181)

23. NRC, NUREG-1409, "Backfitting Guidelines," Washington, DC, July 1990. (ML032230247)

3 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through their Web site: https://WWW.IAEA.Org/ or by writing the International Atomic Energy Agency, P.O. Box 100 Wagramer Strasse 5, A-1400 Vienna, Austria.

4 A copy of this document may be obtained from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Rd, Springfield, VA 22161; telephone: (800) 553-6847, facsimile: (703) 605-6900; e-mail: orders@ntis.fedworld.gov.

BIBLIOGRAPHY

U.S. Nuclear Regulatory Commission Documents

Miscellaneous Office of Nuclear Security and Incident Response documents

Letter dated April 5, 2004, from Roy Zimmerman to Steven Floyd, Vice President of the Nuclear Energy Institute, "establishing implementation standards for the IMP (Safeguards Information) prior to publication of a regulatory guide."