U.S. NUCLEAR REGULATORY COMMISSION December 2015
OFFICE OF NUCLEAR REGULATORY RESEARCH Division 5

DRAFT REGULATORY GUIDE

Technical Lead
Contact: W. Held

DRAFT REGULATORY GUIDE DG-5044 (U)

(Proposed Revision 1 of Regulatory Guide 5.77, dated March 2009)

INSIDER MITIGATION PROGRAM (U)

A. INTRODUCTION (U)

Purpose (U)

(U) This regulatory guide 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 as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55(b)(9)(i).

Applicable Rules and Regulations (U)

- (U) 10 CFR 50.34, "Contents of applications; technical information," (Ref. 1) paragraph (c)(2), states in part that each applicant for an operating license for a utilization facility that will be subject to the requirements of § 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," (Ref. 2) 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."

- (U) 10 CFR 52.79, "Contents of applications; technical information in final safety analysis report," (Ref. 3) paragraph (a)(35)(i), 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.

  - (U) 10 CFR 73.1, "Purpose and Scope," paragraph (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.
  - (U) 10 CFR 73.54, "Protection of digital computer and communication systems and networks," requires that licensees shall provide high assurance that digital computer and

~~NOTICE: The Staff Regulatory Guidance section (Section C of this regulatory guide) contains sensitive unclassified information identified as Official Use Only – Security-Related Information. When Section C is removed from this regulatory guide the remainder of this document is DECONTROLLED.~~

~~DG-5044 is withheld from public disclosure. It is available to those 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) by contacting the Technical Lead for this guide.~~

communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.

- (U) 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," paragraph (b)(7), states that licensees shall establish, maintain, and follow an access authorization (AA) program in accordance with 10 CFR 73.56. Furthermore, 10 CFR 73.55(b)(9)(i) 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.
- (U) 10 CFR 73.56, "Personnel access authorization requirements for nuclear power plants," 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).
- (U) 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," paragraph (2) requires that licensees shall submit fingerprints for those individuals who will have access to Safeguards Information.

- (U) 10 CFR Part 26, "Fitness for Duty Programs," (Ref. 4), in part states, that fitness for duty 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, which in any way adversely affects their ability to safely and competently perform their duties; and the workplaces subject to Part 26 are free from the presence and effects of illegal drugs and alcohol, and 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 Fitness for Duty (FFD) program.

- (U) 10 CFR 50.82, "Termination of license," paragraph (a)(1)(i), requires that when a 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 § 50.4(b)(8).

Related Guidance

- (U) Regulatory Guide (RG) 5.66, "Access Authorization Program for Nuclear Power Plants," (Ref. 5) provides guidance and endorses Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plants Access Authorization Program." The guide describes an approach that the NRC staff has found acceptable in meeting the provisions of 10 CFR 73.55(b)(7) and (b)(9), which requires that an IMP be included as part of the licensee's physical security plan.

- (U) Regulatory Guide (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) (Ref. 6), provides a description of and guidance for mitigating the active insider, and passive insider.

- (U) RG 5.71, "Cyber Security Programs for Nuclear Facilities," (Ref. 7) provides guidance to licensees regarding cyber protection measures,

- (U) NUREG-1959, "Intrusion Detection Systems and Subsystems," (Ref. 8) provides a detailed discussion of proximity sensors, which are used as part of an insider mitigation program.

Purpose of Regulatory Guides (U)

(U) The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides 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 (U)

(U) This regulatory guide contains information collection requirements covered by 10 CFR Part 73, "Physical Protection of Plants and Materials," that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002, 3150-0011, and 3150-0151. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number.

TABLE OF CONTENTS

Purpose (U) 1
Applicable Rules and Regulations (U) 1
Purpose of Regulatory Guides (U) 3
Paperwork Reduction Act (U) 3
Reason for Revision (U) 5
Background (U) 5
Harmonization with International Standards (U) 6
Documents Discussed in Staff Regulatory Guidance (U) ..... **Error! Bookmark not defined.**
1. General Requirements (U) 7
2. Applicability (U) 9
2.1 General Applicability (U) 9
2.2 The Critical Group ~~(OUO-SRI)~~ 10
2.3 Other Personnel for Consideration (U) 11
3. Elements of an Acceptable IMP (U) 12
3.1 Fitness for Duty Elements (U) 12
3.1.1 (U) Drug and Alcohol Testing Provisions 12
3.1.2 Behavioral Observation, § 26.33 (U) 13
3.1.3 Employee Assistance Program, § 26.35 (U) 13
3.1.4 Reporting § 26.717 and §26.719 (U) 13
3.2 Access Authorization Program Elements (U) 13
3.2.1 Initial Security Determination (U) 13
3.2.2 Psychological Assessments, including Medical Evaluations—Initial and Periodic (U) 14
3.2.3 Annual Review by Immediate Supervisor (U) 15
3.2.4 Periodic Reinvestigation of Security Determination (U) 16
3.2.5 Access to Vital Areas (U) 17
3.3 Cyber Security Elements (U) 17
3.4 Physical Protection Plan Elements (U) 18
4. Behavior Observation Training (U) 21
5. FFD Program Elements During Decommissioning (U) 23
GLOSSARY (U) 28
REFERENCES (U) 31

B. DISCUSSION (U)

Reason for Revision (U)

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

(U) 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 permanent removal of fuel from the reactor vessel in accordance with 10 CFR 50.82(a)(1)(i) and 10 CFR 50.82(a)(1)(ii), respectively.

Background (U)

(U) Once an individual has been granted unescorted access to protected areas of a power reactor facility, preventing an adverse event becomes dependent on the insider mitigation program. Defense-in-depth strategies are needed to minimize the potential for an insider to adversely affect, either directly or indirectly, a licensee's ability to safely operate a nuclear facility. This involves detecting an insider threat through the simultaneous application of access controls; behavioral observation, physical protection, drug and alcohol testing, and cyber security. It also involves denial strategies that remove opportunities or prevent the insider from committing a malevolent act by defeating physical protection measures and cyber controls. The licensee's physical protection program must 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 the public health and safety.

(U) The licensee's access authorization (AA) program, FFD program, and Cyber Security Program, in combination with the licensee's Physical Protection Program, provides the fundamental basis for addressing the insider threat. The combined implementation of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," 10 CFR 73.56, "Personnel access authorization requirements for nuclear power plants," 10 CFR 73.55(b)(9)(i), 10 CFR Part 26, "Fitness for Duty Programs," and other requirements such as 10 CFR 73.55(h), provides defense-in-depth to address the insider threat.

The licensee's AA 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, which in any way adversely affects their ability to safely and competently perform their duties. The licensee's cyber security 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 cyber attacks, up to and including the design basis threat (DBT) as described in 10 CFR 73.1. The concurrent and integrated implementation of these programs provides protection to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to provide physical protection of licensed activities against radiological sabotage.

Harmonization with International Standards (U)

(U) The International Atomic Energy Agency (IAEA) has established a series of safety guides and standards constituting a high level of safety for protecting people and the environment. IAEA safety guides present international good practices and increasingly reflect best practices to help users striving to achieve high levels of safety. Pertinent to this regulatory guide, IAEA Nuclear Security Series No. 8, "Preventive and Protective Measures against Insider Threats" (Ref. 9), issued September 2008, provides guidance on prevention of and protection against insider threats. This revision to regulatory guide 5.77 incorporates similar guidelines and is consistent with the basic insider threat mitigation principles set forth in IAEA Nuclear Security Series No. 8.

C. STAFF REGULATORY GUIDANCE (U)

1. General Requirements (U)

~~(OUO-SRI)~~ Insider threats present a unique problem for a physical protection system. Insiders could take advantage of their access rights, complemented by their authority and knowledge of a facility, to bypass dedicated physical protection elements or other provisions such as measures for safety or material control and accounting, including operating measures and procedures. Furthermore, personnel with access in positions of trust acting as insiders are capable of carrying out "defeat" methods not available to outsiders when confronted with protection elements and access controls. Insiders have more opportunities to select the most vulnerable target and the best time to execute a malicious act. This could include, for example, tampering with safety equipment to prepare for an attempt or act of sabotage. A comprehensive IMP is one that is designed to address a broad context of trustworthiness and reliability issues to minimize the potential for adverse actions by an insider. An insider may create an adverse condition other than radiological sabotage that could affect the licensee's ability to respond to a safety or security event that could adversely affect the normal operation of the plant and, therefore, adversely affect the public health and safety and the common defense and security. 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 and mitigate potential adverse acts by insiders

(U) In accordance with 10 CFR 73.55, the Commission has established design requirements for a nuclear power reactor facility physical protection program, including requirements to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage, to prevent significant core damage and spent fuel sabotage. As set forth in 10 CFR 73.55(b)(9)(i), nuclear power reactor licensees are required to establish, maintain, and implement an IMP to monitor the initial and continuing trustworthiness and reliability of individuals granted unescorted access or unescorted access authorization, or retaining unescorted access or 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 AA program described in 10 CFR 73.56; the FFD program described in 10 CFR Part 26; the cyber security program described in 10 CFR 73.54; and, the physical protection program described in 10 CFR 73.55. Licensees must also implement the requirements contained in 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," in order to meet the requirements contained in 10 CFR 73.56(d) and (i).

~~(OUO-SRI)~~ An important focus for an IMP program is the implementation of measures that control personnel access to the licensee's protected areas, vital areas, and accessible target set locations in addition to digital computer, communication systems, and computer networks associated with: safety related and important to safety functions; security functions; emergency preparedness functions, including off site communications; and, support systems and equipment that, if compromised, would adversely impact safety, security, or emergency preparedness functions.

(U) As described in 10 CFR 73.56(a), a licensee is required to establish, implement, and maintain an AA program, as a part of its physical security plan, for granting unescorted access to protected and vital areas of a nuclear power plant. This program's objective 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.

(U) 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 constitute an indication of current or future untrustworthiness or unreliability. These measures will typically provide information that also supports the licensee's IMP.

(U) As described in 10 CFR 73.56(f), "Behavioral observation," 10 CFR 73.56(g), "Self-reporting legal actions," 10 CFR 73.56(i), "Maintaining unescorted access or unescorted access authorization," and 10 CFR 73.56(j), "Access to vital areas," in conjunction with IMP program requirements, licensees are required to ensure, following their initial determination of unescorted access or access authorization, continued trustworthiness and reliability of those with unescorted access to a facility, as well as to maximize opportunities to identify insider activity. Efforts undertaken to ensure the continued trustworthiness and reliability of individuals granted unescorted access also supports the IMP.

(U) Licensees should perform an analysis of their programs and industry or other insider-related events to ensure that their policies, actions, and measures provide a level of protection that meets the IMP requirements. Licensee management, acting as or through a designated reviewing official, may grant, deny, suspend, withhold, revoke, or terminate unescorted access authorization or unescorted access; determine what level of access, if any, an individual will have; and, make all final decisions regarding unescorted access to its facilities in accordance with 10 CFR 73.56, integrated with the performance requirements 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 to retain unescorted access. This 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.

1.1 ~~(OUO-SRI)~~ Licensees are required to implement the requirements contained in 10 CFR 73.54, in conjunction with 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 when the incident is cyber-related. Mitigation of opportunities for insider tampering is particularly important because an insider may have knowledge of how to manipulate various systems in ways that are difficult to detect. Any acts of wrongdoing or overt acts of tampering are particularly serious matters because of the potential adverse impact to the safety and security of the nuclear power plant that could adversely affect the protection of the public health and safety and the common defense and security. The potential for significant harm demonstrates the need for an IMP that ensures the trustworthiness and reliability of specific individuals working at, for, or supporting nuclear power plant operations.

1.2 It is important to recognize that the IMP program alone does not address all cyber threats and attack vectors. As a result, the IMP alone does not take the place of other cyber security

requirements and controls used to mitigate cyber attack vectors and pathways that pose a threat to equipment.

(U) 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 addressing both the intent and capability of the potential insider. Licensees' internal organizations 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 they must implement their IMP programs in a manner that ensures the coordination that provides the defense-in-depth necessary to mitigate the insider threat. An example of this coordination is found in the need for security and human resources personnel to 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 via 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 (U)

(U) The IMP is applicable to individuals assigned to provide defense-in-depth against identified threats or individuals. At a minimum, to mitigate the potential for an insider to be successful, and as directed by the DBT Order, EA-03-086, 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 (certification or unescorted access); (2) initial and random substance abuse testing; (3) psychological assessments, which may include a medical evaluation; (4) review by the immediate supervisor at least annually; and, (5) a security determination conducted by the reviewing official at the conclusion the periodic reinvestigation. For additional guidance, see RG 5.66, "Access Authorization Program for Nuclear Power Plants".

2.1 General Applicability (U)

(U) The IMP applies to all persons who are granted and/or maintain unescorted access or unescorted access authorization to an NRC-licensed power reactor facility. 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 (EOF), as described in Section 2.3 below. Insiders may occupy any position within a licensee's organization, and elements of the IMP apply to all personnel that are in an unescorted access status or are certified for unescorted access authorization. Some disciplines 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 possession of weapons inside the protected area of a licensed facility**.**

2.2 The Critical Group ~~(OUO-SRI)~~

(U) 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 re-established 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, credit history reinvestigation, and a psychological reassessment within 3 years of the date on which these elements were last completed.

(U) As described in 10 CFR 73.56(b) and (i)(1)(v)(B) , the licensee's critical group must include any person who provides the licensee services as described below and performs one or more job functions that are critical to the safe and secure operation of the licensee's facility." The following must be in the critical groups:

(1) (U) All licensed reactor operators.

(2) (U) 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.

(3) (U) Individuals who have extensive knowledge of defensive strategies and design and/or implementation of the plant's defensive strategies, including:

a) (U) site security supervisors,
b) (U) site security managers,
c) (U) corporate security managers (nuclear and applicable contractor security managers),
d) (U) security training instructors.

(4) (U) Individuals in a position to grant an applicant unescorted access or certify unescorted access authorization, including access authorization managers. However, this requirement does not apply to qualified contractors or vendors that certify elements of the access authorization program.

(5) (U) 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, including:

a) (U) plant network systems administrators,
b) (U) IT personnel who are responsible for securing plant networks.

Note: The term "IT personnel" includes: (U)

i. (U) an 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 critical digital assets.

(U) Administrative control: A person with administrative control has the electronic access and rights to independently change either the configuration of a critical digital

asset (CDA) or the cyber security controls in place for a CDA in a manner that could result in an adverse impact to Safety, Important to Safety, Security or Emergency Preparedness (SSEP) functions.

ii. (U) An individual with extensive knowledge of the site-specific cyber-defensive strategy.

Extensive knowledge is defined as having: (U)

a. (U) knowledge of the cyber security controls in place for a CDA;
b. (U) knowledge of how the configuration of a CDA or the cyber security controls can be modified or leveraged in a manner that could result in an adverse impact to SSEP functions;
c. (U) knowledge of vulnerabilities of the site-specific cyber security defensive strategy.

iii. Individuals performing the following functions: (U)

a. (U) site cyber security supervisors;
b. (U) site cyber security manager;
c. (U) site cyber security training manager;
d. (U) corporate cyber security manager;
e. (U) cyber security engineers and administrators;
f. (U) IT personnel who are responsible for authorizing access to CDAs;
g. (U) CDA system administrators;
h. (U) personnel who can independently change the configuration of CDAs or can alter cyber security controls.

iv. (U) Individuals assigned any duty to search for contraband (e.g., weapons, explosives, or incendiary devices).

v. (U) Individuals qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, response team leaders, and armorers.

2.3 Other Personnel for Consideration (U)

~~(OUO-SRI)~~ Licensees may determine that it is desirable to place additional people, 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 the safety and security of the nuclear power facility. For example, those persons who have an "L" or "Q" security clearance, under 10 CFR Parts 11 or 25, respectively, but do not have unescorted access or unescorted access authorization, because they may possess information that could aid an insider.

2.3.1 ~~(OUO-SRI)~~ 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.

2.3.2 (U) The IMP should apply to those persons necessary for the effective implementation of the drug and alcohol testing provisions as described in this guide. These personnel included should be those who are involved in the day-to-day operations of the 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) (U) The FFD coordinator/supervisor responsible for the implementation of the drug and alcohol testing program onsite;

b) (U) Persons in 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) (U) Persons involved in the collection (e.g., collectors if they are licensee employees) or onsite testing of alcohol or urine specimens;

d) (U) Persons, including the Medical Review Officer and site nurse or medical practitioner, if assigned, who:

i. (U) review or take action on EAP findings that represent a concern regarding a licensee or other entities' trustworthiness or reliability determination for an individual(e.g., § 26.35(c)(2)(i));

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

e) (U) Persons who make 10 CFR Part 26, Subpart C, authorization decisions.

2.3.3 (U) The IMP should apply to persons designated to physically report to the EOF and those persons who may have unmonitored access to sensitive (e.g. security- or safety-related) information.

3. Elements of an Acceptable IMP (U)

3.1 Fitness for Duty Elements (U)

3.1.1 (U) Drug and Alcohol Testing Provisions

(U) Section § 73.55(b)(9) requires nuclear power reactor licensees, in part, to include in their IMP elements of the FFD program described in Part 26.

3.1.1.1 (U) The drug and alcohol testing provisions considered adequate for the IMP are those provisions that provide reasonable assurance that individuals are:

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

b. (U) 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.

3.1.1.2 ~~(OUO-SRI)~~ In general, the drug and alcohol testing provisions can be implemented through a licensee's policy and procedures that implement applicable requirements of 10 CFR Part 26, Subparts A through E, G, H, N, and O. At the discretion of the licensee or affected entity, 10 CFR Part 26, Subpart F, "Licensee Testing Facilities,"

may be implemented for initial tests of urine specimens for validity, drugs, and drug metabolites. Additional guidance regarding authorization determinations based on drug and alcohol test results is described in RG 5.66. Licensees shall, as required in 10 CFR 26.189, consider the potential insider threat when making FFD determinations.

3.1.2 Behavioral Observation, § 26.33 (U)

(U) 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 § 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 §§ 26.33 and 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 decommission power.

3.1.3 Employee Assistance Program, § 26.35 (U)

(U) Licensees and other affected entities shall maintain an EAP to strengthen the FFD program by providing confidential assessment, short-term counseling, referral services, and treatment monitoring to individuals who have problems that could adversely affect the individual's ability to safely and competently perform their duties. 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 are provided 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: (i) is likely to cause self-harm or harm to others; (ii) has been impaired from using drugs or alcohol while in a work status and has a continuing substance abuse disorder; or, (iii) has even been engaged in any acts that would be reportable under § 26.719(b)(1) through (b)(3).

3.1.4 Reporting of § 26.717 and § 26.719 (U)

(U) The reporting provisions for Subpart N, "Recordkeeping and Reporting Requirements" are contained in 10 CFR 26.717 and 26.719. Reporting enables effective regulatory oversight of conditions adverse to safety or security and the common defense and security. Trending of this performance information also informs licensee assessment of program implementation and the conduct of NRC inspection to provide assurance that programmatic implementation meets regulatory requirements.

3.2 Access Authorization Program Elements (U)

3.2.1 Initial Security Determination (U)

(U) 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 the latest NRC staff endorsed guidance of NEI 03-01, provide high assurance that persons initially selected for unescorted access or unescorted access authorization 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 (U)

3.2.2.1 (U) 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 as described in paragraph (c) below. 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.

3.2.2.2 (U) 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 physician practitioner in his or her assessment.

(U) As described in 10 CFR 73.56(e), the psychological assessment must include the following:

- (U) 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.
- (U) Predetermined thresholds established for each scale in the test medium in accordance with 10 CFR 73.56(e)(2) must be applied in interpreting the results of the psychological test to determine if an individual must be interviewed by a licensed psychiatrist or psychologist. 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, then the psychological assessment must include a clinical interview. The initial and periodic assessment should have the additional focus of careful consideration of the psychopathology of the interviewee. Psychiatrists or clinical psychologists with the appropriate clinical training and experience should carefully apply procedures of evaluation assessment and diagnosis derived from scientific research.
- (U) 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 significant defect in the trustworthiness, reliability, or judgment of the individual. 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 judgment to the extent that trustworthiness and reliability are jeopardized. Individuals identified as candidates for further medical review should be referred to a physician for further evaluation. 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.

(U) Pursuant to 10 CFR 73.56(i)(1)(v)(B), the psychological assessment must be conducted at intervals not to exceed once every 5 years for individuals in a critical group. Interviews used in the assessment should be conducted in a semi structured manner and include the recognition of medical conditions that could result in impaired judgments or could adversely impact the fitness for duty 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.

3.2.2.3 (U) The interviewing psychiatrists or clinical psychologists with the appropriate clinical training and experience should incorporate the most recent supervisory review, or interview as applicable, as one measure of the assessment.

(U) If in the course of conducting the psychological assessment the licensed psychologist or psychiatrist identifies or discovers any information, including a medical condition, that could adversely impact the fitness for duty 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.

(U) As described in 10 CFR 73.56(i), licensees shall take appropriate action, in accordance with established site procedures, if disqualifying information is provided as a result of a psychological assessment, to administratively withdraw unescorted access for any worker who has not met the psychological reassessment criteria.

3.2.3 Annual Review by Immediate Supervisor (U)

(U) A review conducted by the assigned supervisor has value as an integral part of the behavior observation program (BOP) 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 has the opportunity to become cognizant 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.

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

3.2.3.1 (U) In some cases, the supervisor may not have frequent enough personal interaction with the individual throughout the review period needed to develop an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability. When this unusual condition occurs, the interview may consist of face to face contact, in addition to 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 individuals continued trustworthiness and reliability. In addition, the licensee must ensure that the annual supervisory review or interview is conducted consistent with the requirements of 10 CFR 26.27, "Written Policy and Procedures," and 10 CFR 26.29, "Training."

3.2.3.2 (U) The supervisory review may be satisfied by incorporating information developed over the covered period (i.e., annually) regarding 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 BOP, as well as those deviations from the behavioral norm 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 (U)

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

~~(OUO-SRI)~~ Under 10 CFR 73.56(i)(1)(v)(B)(1) through (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. Members of the critical group must also get a psychological reassessment within 5 years of the date on which this assessment was last completed. The requirements of this section apply to all individuals with unescorted access authorization or unescorted access who are members of the critical group. Individuals who have not satisfied the reinvestigation requirements shall have unescorted access authorization or unescorted access administratively withdrawn until the reinvestigation has been completed, or the worker should be reassigned to non critical group positions until the required critical group reassessment can be completed.

The reinvestigation shall include the following: (U)

- (U) A review of 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.
- (U) 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 Federal Credit Reporting Act disclosure and authorization statement forms before initiating this reinvestigation.
- (U) Licensees shall take appropriate action if disqualifying information is discovered during any reinvestigation review.

- (U) 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 (U)

(U) 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 will be updated and reapproved at least every 31 days to minimize insider threats by ensuring that personnel listed have a continued need to access vital areas to perform their official duties and not just a possibility of needing access sometime in the future. The list must include only those individuals who have a continued need for unescorted access to those specific vital areas in order to perform their routine 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.

(U) The intent of this requirement is to minimize 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. Licensees must ensure that persons who are directing the work activity of persons with unescorted access, or are responsible for fulfilling behavior observation requirements of persons with unescorted access, recertify the continued need for vital area unescorted access no less frequently than at a 31 day frequency. 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 a licensee's vital areas.

3.2.5.1 (U) 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 are required 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 Cyber Security Elements (U)

~~(OUO-SRI)~~ Licensees must ensure that cyber protection measures have been established as required in 10 CFR 73.54 and articulated in RG 5.71, "Cyber Security Programs for Nuclear Facilities". In particular, licensees should consider the following for IMP implementation:

- (U) access control,
- (U) audits and accountability,

- (U) system and communication protection,
- (U) identification and authentication,
- (U) personnel security, and
- (U) awareness and training.

3.3.1 (U) Additional guidance on each of these topics is available to licensees and applicants in Regulatory Guide 5.71.

3.3.1.1 (1) Appendix B, Technical Security Controls (U)

(U) B.1.10 Session Lock
(U) B.3.2 Application Partitioning and Security Function Isolation
(U) B.3.6 Transmission Integrity
(U) B.3.7 Transmission Confidentiality
(U) B.4.2 User Identification and Authentication, and
(U) B.4.5 Device Identification and Authentication

3.3.1.2 Appendix C, Operational and Management Security Controls (U)

(U) C.3.6 Security Functionality Verification
(U) C.11.3 Baseline Configuration
(U) C.11.6 Access Restrictions for Change, and
(U) C.11.7 Configuration Settings

~~(OUO-SRI)~~ Licensees should conduct random patrols, by trained staff, of CDAs that affect SSEP functions to look for obvious signs of cyber related tampering.

3.4 Physical Protection Plan Elements (U)

3.4.1 (U) Licensees should have procedures available for operator response to events involving deliberate acts directed against plant equipment. For additional information see the below references:

(U) The NRC has issued two information notices (INs) to address conditions that could be potential insider threats. On May 4, 1983, the NRC published IN 83-27, "Operational Response to Events Concerning Deliberate Acts Directed against Plant Equipment" (Ref. 10), in which the NRC provided licensees with information necessary for the

formulation of programmatic activities that licensees could consider to prepare for and respond to insider directed behaviors.

(U) 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 information notice stated, 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.

(U) On December 27, 1996, the NRC published IN 96-71, "Licensee Response To Indications Of Tampering, Vandalism, Or Malicious Mischief" (Ref. 11). IN 96-71 provides additional information for licensees to consider beyond the information provided in IN 83-27 in the form of examples of known and unexplained conditions that were inconsistent with routine operations, and it reminded licensees that events of the nature described in the IN are required to 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 ~~(OUO-SRI)~~ In considering program elements needed to mitigate the active insider and active violent insider, licensees should develop a program that will:

a) ~~(OUO-SRI)~~ Ensure licensed operators are properly trained to recognize indications of tampering, which includes prepositioning of equipment, to report such conditions in a timely manner, and to compensate for degraded conditions as appropriate.

b) ~~(OUO-SRI)~~ Ensure armed security officers are properly trained to recognize obvious indications of tampering as required in 73.55(i)(5)(vii), and Part 73, Appendix B, Section D.1.(b)(1).

c) ~~(OUO-SRI)~~ Ensure personnel who receive plant access training are trained to recognize behaviors or conditions adverse to safe operations and security of the facility.

d) ~~(OUO-SRI)~~ Develop procedures and training requirements to react effectively to conditions related to actual or suspected tampering as required in 73.55(i)(5)(viii).

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

f) ~~(OUO-SRI)~~ Conduct random armed patrols of target set equipment or elements as required in 73.55(i)(5)(vi).

3.4.3 (OUO-SRI) The program should identify, and provide training to address, target set equipment or elements that:

a) ~~(OUO-SRI)~~ could be disabled locally,

b) ~~(OUO-SRI)~~ would not be observable from remote indications (e.g., the control room),

c) ~~(OUO-SRI)~~ 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 relative susceptibility to tampering.

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

e) ~~(OUO-SRI)~~ Licensees should train operations personnel to be sensitive to abnormalities that could be the result of tampering and to respond to such indications in a timely manner. During routine tours, operations personnel should be sensitive to changes in configurations that might indicate possible tampering. Licensees should review, determine, and provide training to 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 prior to operation.

f) ~~(OUO-SRI)~~ 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 targets set equipment or elements , except where precluded by immediate personnel safety concerns, operational abnormalities, or restrictions, consistent with guidelines to keep radiation dose rates as low as reasonably achievable.

g) ~~(OUO-SRI)~~ As described in 10 CFR 73.55(i)(5)(viii), licensee security plans and implementing procedures shall describe the operations and security response to actual tampering events. Any suspected tampering event should be entered into the licensee's corrective action program, and reported as required by 10 CFR 73.71.

h) ~~(OUO-SRI)~~ 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. NEI 03-12, describes the specifics of a patrol program that the NRC has found acceptable.

i) ~~(OUO-SRI)~~ Licensees may substitute surveillance and tamper detection mechanisms for armed patrols if these mechanisms can provide notification to 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 employed 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" (Ref. 12), 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." Armed patrols and surveillance mechanisms should provide for notification to 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, "Intrusion Detection Systems and Subsystems," issued March, 2011 provides a detailed discussion of proximity sensors. Section 4.4.4, "Characteristics and Applications," provides licensees with detailed information regarding implementation options.

j) ~~(OUO-SRI)~~ Licensees should ensure that searches are performed in accordance with 10 CFR 73.55(h) such that searches will ensure personnel are searched for contraband (weapons, explosives or incendiary devices) before entering the facility. This makes contraband searches an integral physical protection element of the IMP.

4. Behavior Observation Training (U)

4.1 ~~(OUO-SRI)~~ A comprehensive and effective BOP will include a training program for recognizing and reporting behaviors as required in § 73.56(f)(3), which may be considered adverse to the safe operation and security of the licensee facility.

4.2 ~~(OUO-SRI)~~ Licensees should ensure that the BOP training includes recognition of and response to the following conditions or behavioral characteristics:

- (OUO-SRI) the recognition that changes in emotional state can happen quickly;
- ~~(OUO-SRI)~~ typical conditions that can trigger behavioral anomalies;
- ~~(OUO-SRI)~~ the need for early intervention after the recognition of changes in behavior that typically indicate changes in emotional state;
- ~~(OUO-SRI)~~ the recognition of uncharacteristic deviations in coworker interactions, uncharacteristic absences from work, uncharacteristic inattention to detail, or suspected alcohol or drug abuse;
- ~~(OUO-SRI)~~ individual(s) seeking information about security of the facility not provided through normal means (e.g., training programs), including unusual interest in, or predisposition toward, security;
- ~~(OUO-SRI)~~ individual(s) eliciting information regarding operational activities outside the scope of an individual's normal work assignments (e.g., questioning of other persons at a level beyond mere curiosity about particular facets of a facility, or purpose of a structure, its operations, security procedures, etc.) in a manner that would arouse suspicions in a reasonable person;
- ~~(OUO-SRI)~~ individual(s) disappearing from a work assignment without adequate explanation or frequent or unexplained absence(s) from work assignments;
- ~~(OUO-SRI)~~ individual(s) unsatisfactory response when questioned about their work activities (e.g., unusual or inadequate response when confronted about being in a plant or office location outside of the worker's usual scope of work);
- ~~(OUO-SRI)~~ individual(s) vocalizing actual or potentially threatening views or opinions that could be threatening to a nuclear facility;

- ~~(OUO-SRI)~~ individual(s) in any plant area where they may not belong (e.g., an individual in an area outside of his usual scope of activities who cannot provide an appropriate explanation for being in the location);

- ~~(OUO-SRI)~~ suspicious circumstances that cannot be explained through operational means, (e.g., abnormalities that could be vandalism or tampering). Examples include but are not limited to:

    a) ~~(OUO-SRI)~~ misaligned breakers or valves,

    b) ~~(OUO-SRI)~~ cut wires or cables,

    c) ~~(OUO-SRI)~~ foreign objects in machinery, reservoirs, or tanks,

    d) ~~(OUO-SRI)~~ 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;

- ~~(OUO-SRI)~~ behavior that appears to challenge installations, buildings, or systems, including cyber security capabilities;

- ~~(OUO-SRI)~~ taking pictures or video of sensitive facilities without pre-authorization, or recording personnel activities, buildings, or infrastructure in a manner that would arouse suspicions in a reasonable person. Examples include 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.);

- ~~(OUO-SRI)~~ individual(s) demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional interest such that a reasonable person would consider the activity suspicious. Examples include unusual observation through binoculars, questionable note-taking, attempting to measure distances, etc., that have no apparent nexus to facility operations;

- ~~(OUO-SRI)~~ possession of unusual quantities of cell phones, pagers, etc., such that a reasonable person would suspect criminal activity;

- ~~(OUO-SRI)~~ 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;

- ~~(OUO-SRI)~~ unusual interest in an organization's technology infrastructure;

- ~~(OUO-SRI)~~ 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;

- ~~(OUO-SRI)~~ the need to report any of the above conditions to the employee's assigned supervisor or FFD program manager or access authorization program manager.

5. FFD Program Elements During Decommissioning (U)

(U) Licensees must continue to meet the requirements of 10 CFR 73.55(b)(9) following the licensee's submission of its certification to cease operations as described in 10 CFR 50.82(a)(1)(i), and its certification for permanent fuel removal as described in 10 CFR 50.82(a)(1)(ii), throughout decommissioning until the Commission has terminated the license as described in 10 CFR 50.82. This includes implementing elements of 10 CFR Part 26 (Subparts A through E, G, H, N, and O, and F at the discretion of the licensee or affected entity for initial tests of specimens for validity, drugs, and drug metabolites), as described in paragraph 3.1.1 above and as specified in 10 CFR 73.55(b)(9)(ii)(B). Although the requirements of Part 26 are applicable only to "reactors authorized to operate," see 10 CFR 26.3, many elements of Part 26 are necessary elements of the IMP and must continue to be met in order to ensure trustworthiness and reliability of individuals granted or retaining unescorted access or unescorted access authorization to a protected or vital area as required by both 10 CFR 73.56 and 10 CFR Part 26.

5.1 (U) The NRC acknowledges that some drug and alcohol testing provisions are not necessary to ascertain whether an individual is trustworthy and reliable. These provisions are provided below.

(U) Table 1 – Drug and Alcohol Testing Provisions not associated with Trustworthiness and Reliability

	Drug and Alcohol Provisions	Reference Requirement
a	Performance Objectives	§ 26.23(e)
b	Audits and Corrective Actions	§ 26.41(c)(1) and (2) (Note 1); and (e) (Note 2)
c	Collection Sites, Preparation, and Testing	§§ 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	§ 26.167 (Note 4)
e	Blind Performance Testing	§ 26.168 (Note 4)
f	FFR Program Performance Data	§ 26.717(b)(9) (Note 5)
g	Reporting requirements	§ 26.719(c) (Note 6)

(U) Note 1 – Auditing of a blind performance specimen provider and the primary and secondary U.S. Department of Health and Human Services' (HHS)-certified laboratories is not an element of 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, 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 that: (1) the laboratories and the BPTS supplier process/provide specimens, respectively, from/to at least one other NRC licensee in accordance with Part 26 and are subject to the § 26.41 audit requirement; (2) at least one other operating reactor's audit report is shared with the decommissioning licensee; and (3) significant performance issues have not been identified. 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 Part 26 program effectiveness (e.g., procedure issues, failure to conduct limit of detection testing, blind or quality control specimen failures, see Note 4 below) and adequate corrective actions were not implemented by the laboratory or PBTS supplier to preclude recurrence. Audits can be conducted with those conducted 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 who has submitted its § 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.

(U) 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/technician responsible for FFD program implementation, including drug and alcohol testing, may audit the offsite collection facility, laboratory, and blind sample supplier.

(U) Note 3 – The use of a collection facility meeting the requirements of § 26.87 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 if the § 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 § 26.87 or 49 CFR Part 40, except if the licensee implements a short-duration transition period (e.g., less than 90 days) when shifting from an onsite to offsite collection facility.

(U) Note 4 – The quality assurance and quality control (QA/QC) and blind performance specimen testing provisions are not elements of Part 26 necessary to determine the trustworthiness and reliability of individuals subject to the IMP; however, these requirements do provide assurance that laboratories and BPTS suppliers are performing acceptably. As a result, the licensee should on an annual basis verify that: (1) both laboratories process QA/QC and blind samples from at least one other NRC licensee in accordance with 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 Part 26 program effectiveness (e.g., a procedure issue, failure to confirm, a § 26.719 reportable event) and adequate corrective actions were not implemented by the laboratory or BPTS supplier to preclude 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 who has submitted its § 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 back-up HHS-certified laboratories and BPTS supplier.

(U) Note 5 – The fatigue management provisions of 10 CFR Part 26, Subpart I, are not elements of 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.

(U) Note 6 – The reporting requirements of § 26.719(c)(1)-(3), except for the Medical Review Officer and random testing error provisions, are not applicable unless the licensee decides to

conduct QA/QC and BPTS performance testing and discovers reportable errors associated with the testing of their specimens.

D. IMPLEMENTATION (U)

(U) The purpose of this section is to provide information on how applicants and licensees[1] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with 10 CFR 50.109, "Backfitting," and any applicable finality provisions in 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

Use by Applicants and Licensees (U)

(U) Applicants and licensees may voluntarily[2] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

(U) Licensees may use the information in this regulatory guide for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59, "Changes, Tests, and Experiments." Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

(U) Licensees may commit in their physical security plan to using the guidance in this regulatory guide. Because a licensee's physical security plan is part of its licensing basis, the regulatory guide will become a part of a licensee's licensing basis and, as a part of its license, a requirement upon the licensee. Licensees that amend their security plans to commit to this version of RG 5.77 should specify that they consider the permissive elements of the guidance that use the term "should" to be requirements.

Use by NRC Staff (U)

(U) For those licensees that do not adopt this regulatory guide into their licenses, the NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect or plan to request these licensees to voluntarily adopt this regulatory guide to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action that would require the use of this regulatory guide without further backfitting consideration. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide.

(U) During regulatory discussions on plant specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, as one acceptable means

---

1 In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52.

2 In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this regulatory guide are part of the licensing basis of the facility. However, if this regulatory guide becomes part of the licensing basis for a facility, the staff may represent to that licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation of its license.

(U) If an existing licensee that does not adopt this regulatory guide into its licensing basis voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this regulatory guide and (2) the specific subject matter of this regulatory guide is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

(U) Additionally, an existing applicant may be required to comply with new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

(U) If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409, "Backfitting Guidelines" (Ref. 13) and the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 14).

GLOSSARY (U)

(U) 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, impedes a response to the threat).
(U) 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.
(U) administrative withdrawal of UAA/UA	A process to temporarily withhold unescorted access authorization (UAA)/unescorted access (UA) from an individual while action is taken to complete or update an element of the UAA requirements.
(U) annual	Requirements specified as "annual" should be scheduled at a 12-month periodicity.
(U) 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 their Physical Security Plan, prior to receiving their operating licenses or the Commission finding under 10 CFR 52.103(g).
(U) background investigation (BI)	Information from all BI elements to be collectively evaluated by the reviewing official pursuant to a determination of trustworthiness and reliability of an individual. Depending upon the BI period, the BI 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.
(U) behavior observation program (BOP)	An awareness program that meets requirements of both the access authorization and FFD programs. Personnel are trained to report legal actions; to possess certain knowledge and abilities related to abuse of 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.
(OUO-SRI) critical group	Any individual who performs job functions critical to the safe and secure operation of the licensee's facility. This individual includes any individual who has been granted UA or certified UAA and performs one or more of the following job functions:

a. ~~(OUO-SRI)~~ any individuals who have extensive knowledge of facility defensive strategies or who design or implement the plant's defense strategies;

b. ~~(OUO-SRI)~~ any individuals in a position to grant an individual unescorted access or to certify an individual unescorted access authorization;

c. ~~(OUO-SRI)~~ any individuals assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices);

d. ~~(OUO-SRI)~~ any individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in 10 CFR 73.54.

(U) Fitness for Duty Authorization (FFDA)	A term commensurate with "authorization" as defined in 10 CFR 26.5, "Definitions." An element of UAA that identifies the status of an individual's required FFD elements, which are then evaluated by a reviewing official to determine whether the individual is trustworthy, reliable, and fit for duty.
(U) insider	A person who has been granted unescorted access or unescorted access authorization under the requirements of 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," 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.
(U) passive insider	A person who provides or attempts to provide safeguards or other relevant information regarding a licensee's physical configurations, designs, strategies, or capabilities to any person who does not have a functional or operational need to know.
(U) 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.
(U) reinvestigation	A periodic inquiry or assessment conducted to ensure that individuals continue to meet UAA or UA or fitness for duty program suitability requirements as defined in the most current NRC staff endorsed version of NEI 03-01, which describes an approach that the U.S. NRC staff has found acceptable.
(U) reviewing official	The licensee or, if applicable, the contractor or vendor, persons designated by their company to be responsible for reviewing and evaluating all data collected about an individual, including potentially disqualifying information, in order to determine whether the individual may be authorized UAA or granted UA.
(U) semi-structured interview	An interview with an individual applying for UAA or a person maintaining UAA, conducted by a psychiatrist or a licensed psychologist with clinical experience as required by applicable state requirements, containing 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.
(U) 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.
(U) target set	The combination of equipment or operator actions which, 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, non-localized fuel melting, or core disruption), barring extraordinary action by plant operators. A target set with respect to spent fuel sabotage is equipment that can be manipulated to facilitate draining the spent fuel pool, leaving the spent fuel uncovered for a period of time, allowing spent fuel heat up and the associated potential for release of fission products.
(U) unescorted access (UA)	Status granted to an individual after satisfactorily completing all regulatory requirements for UAA and FFDA, and the individual has completed plant access training; is subjected to a behavioral observation program; is placed in a random drug and alcohol testing program; and is provided the physical means to gain UA to the protected area.
(U) unescorted access authorization (UAA)	Status in the access authorization process after the individual satisfactorily completes all required elements as specified in Section 6 (including the FFDA elements: consent, self-disclosure, suitability inquiry, drug and alcohol testing elements defined in 10 CFR Part 26, "Fitness for Duty Programs," being subject to a BOP and training in the FFD knowledge and abilities),which were evaluated by a licensee reviewing official who then made a favorable determination relative to the individual's trustworthiness, reliability, and fitness for duty.
(U) OUO-SRI	Official Use Only—Security-Related Information.

REFERENCES[3] (U)

1. *U.S. Code of Federal Regulations* (CFR), "Contents of applications; technical information," Part 50, Chapter 1, Title 10, "Energy"

2. CFR, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," Part 73, Chapter 1, Title 10, "Energy"

3. CFR, "Contents of applications; technical information in final safety analysis report," Part 52, Chapter 1, Title 10, "Energy"

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

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

6. (U) NRC, Regulatory Guide (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.

7. (U) NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

8. (U) NRC, NUREG-1959, "Intrusion Detection Systems and Subsystems," Washington, DC.

9. IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) Vienna, Austria, 2011."[4]

10. (U) NRC, Information Notice 83-27, "Operational Response to Events Concerning Deliberate Acts Directed against Plant Equipment," Washington, DC. (ADAMS No. ML082831453)

11. (U) NRC, Information Notice 96-71, "Licensee Response to Indications of Tampering, Vandalism, or Malicious Mischief," Washington, DC December 27, 1996. (ADAMS No. ML031050461)

---

3 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. 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; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov. Documents that are withheld from the public could 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).

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

12. (U) Sandia Report SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," September 2007. [5]

13. (U) NRC, NUREG-1409, "Backfitting Guidelines," July 1990, NRC, Washington, DC. (ADAMS No. ML032230247)

14. (U) NRC, Management Directive (MD) 8.4, "Management of Facility-Specific Backfitting and Information Collection," October 2013, NRC, Washington, DC.

5 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, Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

BIBLIOGRAPHY

U.S. Nuclear Regulatory Commission Documents

Miscellaneous NSIR Documents

Letter dated April 5, 2004, from Roy Zimmerman to Steven Floyd, Vice President of NEI, "establishing implementation standards for the IMP (Safeguards) prior to publication of a regulatory guide." (SGI) [6]

6 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. 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; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail pdr.resource@nrc.gov. Documents that are withheld from the public could 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).