U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

March 2009

Division 5

REGULATORY GUIDE

REGULATORY GUIDE 5.77

(Draft was issued as DG-5011, dated December 2008)
(New Regulatory Guide)

INSIDER MITIGATION PROGRAM

A. (U) INTRODUCTION

(U) This guide describes an approach that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for an insider mitigation program (IMP) at nuclear power reactor facilities. Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," specifically paragraph (b)(7) states that licensees shall establish, maintain, and follow an access authorization program in accordance with 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants." The licensee's physical security plan must include descriptions of the access authorization program and the IMP. Furthermore, pursuant to 10 CFR 73.55(b)(9), licensees shall design and implement the IMP to oversee and monitor the initial and continuing trustworthiness and reliability of individuals granted unescorted access or retaining unescorted access authorization to a protected or vital areas. The IMP should use defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage or spent fuel sabotage.

(U) This document provides guidance for an IMP that would meet the requirements in 10 CFR 73.55(b)(7) and (b)(9) and the latest NRC staff endorsed version of the industry's guidance document, Nuclear Energy Institute (NEI) 03-01, "Nuclear Power Plant Access Authorization Program." These sources provide an acceptable approach for an IMP that meets the provisions of 10 CFR 73.55 as part of the licensee's physical security plan. These sources are also consistent with the guidance described in this regulatory guide.

(U) The NRC issues regulatory guides to describe and make available the methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. 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 finding required for the issuance or continuance of permit or license by the Commission.

(U) This guide was issued after consideration of comments received from stakeholders.

(U) Regulatory guides are issued in 10 broad divisions-1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

(U) This regulatory guide contains guidance on how licensees should implement an IMP. Licensees may employ methods other than those described herein for meeting the Commission's regulations if the chosen measures satisfy the stated Commission requirement(s). The approaches and examples described in this regulatory guidance provide one methodology for satisfying the Commission's requirements for an IMP at nuclear power reactor facilities.

(U) Licensees with operating reactors licensed under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," can apply the guidance in this regulatory guide before fuel is allowed on site (protected area).

(U) Any information collection activities mentioned in this regulatory guide are included as requirements in 10 CFR 73.8, "Information Collection Requirements," which provides the regulatory basis for this guide. The NRC considers the guidance contained in this document to be the most current concerning acceptable approaches.

(U) The NRC issues regulatory guides to describe 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.

(U) This regulatory guide relates to information collection requirements covered by 10 CFR Part 73, and that the Office of Management and Budget (OMB) approved under OMB control number 3150-0002. 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.

B. (U) DISCUSSION

(U) Because of changes to the threat environment after the events of September 11, 2001, the Commission began reevaluating physical protection program requirements at nuclear power reactor facilities. This changing threat environment resulted in several significant protection and regulatory enhancements to ensure that licensees maintain the capability to provide high assurance of the health and safety of the public against the design-basis threat (DBT). Specifically, the provisions of 10 CFR 73.1, "Purpose and Scope," describe how an insider might cause or assist in radiological sabotage. Furthermore, in a Commission order dated April 29, 2003 (EA-03-086), the NRC required licensees to address the insider threat. Pursuant to this order, licensees updated their site security plans to specify how they will comply with the requirements of 10 CFR 73.1 and the DBT order.

(U) A licensee's access authorization program, fitness-for-duty program, and behavior observation program (BOP) provide the framework for addressing the insider threat. Once an individual has been granted unescorted access to protected and vital areas of a power reactor facility, preventing an adverse event becomes dependent on detecting the insider through one of these programs and/or by denying the undetected insider the opportunity to commit the act by other means, such as physical and cyber protective security measures, as appropriate. Performance-based program requirements are intended to generically satisfy the minimum level of performance that a licensee's physical protection program must achieve to provide adequate protection and minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage or spent fuel sabotage.

(OUO-SRI) Pursuant to 10 CFR 73.55(b)(7) and (b)(9), which provide the necessary flexibility for licensees to address the complexities of an insider threat, the NRC staff has nonetheless established the minimum criteria required to meet the DBT goal of mitigating the active insider, active violent insider, or passive insider in Section C of this guide.

(b)(7)(F)

(U) The IMP elements are 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 or could affect the normal operation of the plant. Licensees should consider, and be sensitive to, subtle changes in an individual's behavior or actions over time and use appropriate IMP elements (e.g., behavioral observation program) to assess and mitigate potential adverse acts by insiders.

(U) A trusted person with protected or vital area access, or access to digital computer and communications systems and networks from outside the protected area, can pose a significant threat to the safety and security of a nuclear power plant. Licensees may be unable to identify the cause of incidents that are indicative of potential tampering, which makes it difficult to conclusively determine if a condition

that was discovered was the result of tampering. Irrespective of whether security events involve acts that are within the scope of 10 CFR 73.1 and the DBT, acts of malfeasance or tampering are particularly serious matters because of the potential adverse impact to the safety and security of the nuclear power plant. These events demonstrate the need for an IMP that ensures the trustworthiness and reliability of specific individuals working for or supporting a nuclear power plant.

(U) The broad spectrum of issues related to insider threats ranges from the premeditated actions of an individual acting as a single source of origin, to events that might be sufficient to motivate someone to act, such as extortion. The highly unpredictable threat requires a comprehensive approach to addressing both the intent and capability of the potential insider. Licensee internal organizations should coordinate to provide the defense-in-depth necessary to mitigate the insider threat. An example of this is the need for security and human resources personnel to work closely with employee assistance program (EAP) personnel to ensure that an individual demonstrating the potential to harm themselves or others is 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.

C. (U) REGULATORY POSITION

1. (U) General Requirements

(U) In accordance with Title 10 of the *Code of Federal Regulations* Part 73 (10 CFR 73), "Physical Protection of Plants and Materials," Section 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," the Commission has established design requirements for a nuclear power reactor facility physical protection program, including the performance criteria to detect, assess, interdict, and neutralize threats up to and including the DBT of radiological sabotage, thereby preventing significant core damage and spent fuel sabotage. Under 10 CFR 73.55(b)(7) and(b)(9), licensees shall establish, maintain, and implement an access authorization program and IMP in accordance with 10 CFR 73.56 and describe the programs in their physical security plans. The IMP must be designed and implemented to oversee and monitor the initial and continuing trustworthiness and reliability of individuals granted unescorted access 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, a licensee's capability to prevent significant core damage or spent fuel sabotage.

(U) In 10 CFR Part 73, "Physical Protection of Plants and Materials," Section 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," a licensee is required to establish and implement a 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) This document contains guidance for an acceptable IMP that would meet the requirements of 10 CFR 73.55(b)(7) and (b)(9). Furthermore, the latest NRC staff endorsed version of NEI 03-01 also describes an approach that the NRC staff has found acceptable in meeting the provisions of 10 CFR 73.56 with respect to an IMP as part of the licensee's physical security plan, and is consistent with the guidance described in this regulatory guide.

2. (U) Elements of an Acceptable Insider Mitigation Program

(U) Threat is a function of intent and capability. To provide defense-in-depth against threats, a licensee should establish an IMP that will address both the human reliability factors associated with intent and physical protection measures to mitigate the capability of a potential insider to commit an adverse act.

(U) As a minimum to mitigate the potential for an insider, an IMP should consist of the following elements for all personnel with unescorted access authorization to the protected and vital areas of a facility: (1) a security determination (clearance or access authorization); (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; (5) a security determination of the periodic reinvestigation.

2.1 (U) Insider Mitigation Program Elements-Critical Group

2.1.1 (U) *Participation*

(U) Though 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 authorization status, some groups are considered to have a higher potential for insider threat (i.e., greater capability) because of their

knowledge, access to, or possession of weapons inside the protected area of a licensed facility. Pursuant to 10 CFR 73.56(i)(1)(v)(B), for any individual in the critical group the trustworthiness and reliability determination must be based on a criminal history update and credit history re-investigation within 3 years of the date on which these elements were last completed, or more frequently, based on job assignments as determined by the licensee or applicant and a psychological re-assessment within 5 years of the date on which this element was last completed:

Individuals who perform one or more of the following job functions must be in the critical group:

- All licensed reactor operators.
- 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.
- Individuals who have extensive knowledge of defensive strategies and design and/or implementation of the plant's defensive strategies, including:
    - site security supervisors
    - site security managers
    - corporate security managers (nuclear and/or applicable contractor security managers)
    - security training instructors
- Individuals in a position to grant an applicant unescorted access or unescorted access authorization, including assess authorization managers. However, this requirement does not apply to qualified contractor/vendors (C/Vs) that certify elements of the access authorization program.
- Individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in 73.54, including:
    - plant network systems administrators
    - IT personnel who are responsible for securing plant networks
      Note: the term "IT personnel" should also consider personnel who have the ability and access to change the configuration of control systems (e.g., Supervisory Control and Data Acquisition (SCADA) systems) or other systems that use embedded devices (e.g., Electronically Erasable Programmable Read-Only Memory (EEPROMs)).
- Individuals assigned a duty to search for contraband (e.g., weapons, explosives, or incendiary devices).
- Individuals qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, response team leaders, and armorers.

(b)(7)(F)

(b)(7)(F)

(U) The decision to include additional personnel in the critical group should be based on the licensee's IMP goals and performance objectives associated with mitigating Active Insiders (AI), Active Violent Insiders (AVI), and Passive Insiders (PI). However, those personnel referenced under 10 CFR 73.56(i)(1)(v)(B), must be included in the IMP. The NRC staff's policy concerning the insider during security performance evaluation testing is contained in 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."

2.1.2 (U) *Initial Security Determination*

(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, "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees," 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.

2.1.3 (U) *Drug and Alcohol Testing—Pre-access, Random, For cause, Post-event, and Followup*

(U) Drug and alcohol testing is an important element of the access authorization and fitness-for-duty programs. Pre-access, random, for cause, post event, and followup testing provides a deterrent that supports both safety and security and reinforces the fundamental concepts of trustworthiness and reliability.

(U) The ***Pre-access, Random, For cause, Post-event, and Followup*** drug and alcohol testing element of an IMP may be implemented by applying the guidance for meeting the requirements of 10 CFR Part 26, "Fitness for Duty Programs," and the latest NRC staff endorsed guidance described in NEI 03-01, "Nuclear Power Plant Access Authorization Program."

2.1.4 (U) *Psychological Assessments including Medical Evaluations—Initial and Periodic*

(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.

(U) The psychological assessment must include the following:

a. **(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.

b. **(U)** Predetermined thresholds established for each scale in accordance with 10 CFR 73.56(e)(2) must be applied in interpreting the results of the psychological test to determine whether an individual shall 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 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.

c. **(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 requirements 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.

(U) Prior to any psychological or medical assessment, the physician practitioner should review a current position description of the person being interviewed and the most recently completed supervisory review, if applicable and if the review contains information that could assist the physician practitioner in their assessment.

(U) The interviewing psychiatrists or clinical psychologists with the appropriate clinical training and experience should incorporate the most recent supervisory review 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, based on standards identified in the regulation, who currently has unescorted access or unescorted access authorization status, 10 CFR 73.56(e)(6) requires that he or she 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 under the requirements of 10 CFR Part 26.

(U) Licensees shall take appropriate action, in accordance with procedures, if disqualifying information is provided as a result of a psychological assessment or to administratively withdraw unescorted access for any worker who has not met the psychological reassessment criterion.

2.1.5 (U) ***Annual Review by Immediate Supervisor***

(U) A review conducted by the assigned supervisor has value as an integral part of the 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.

In some cases, the supervisor may not have frequent enough interaction with the individual throughout the review period needed to form an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability. In this situation, the individual is also subject to an annual supervisory review in accordance with the requirements of the licensee's or applicant's BOP. The interview may consist of: face-to-face contact, gathering of information from personnel who have frequent interaction with the individual, or other documented methods of gathering information to ensure the supervisor can attest to the individuals continued trustworthiness, and reliability. Additionally, the licensee should provide appropriate initial training of newly assigned supervisors and annual combined supervisory/worker refresher training. This process should be defined in licensee procedures and policies.

(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 objective of 10 CFR Part 26. Second, it can identify issues related to trustworthiness and reliability.

2.1.5. a BOP Training

Licensees should ensure that the BOP training includes: (1) the recognition that changes in emotional state can happen quickly; (2) typical conditions that can trigger behavioral anomalies; (3) the need for early intervention after the recognition of changes in behavior that typically indicate changes in emotional state; (4) the recognition of uncharacteristic deviations in co-worker interactions, uncharacteristic absences from work, uncharacteristic inattention to detail, or suspected alcohol or drug abuse; and (5) the need to report the above conditions to the employee's assigned supervisors or fitness-for-duty program manager.

2.1.6 (U) ***Periodic Reinvestigation of Security Determination***

(U) Pursuant to 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 re-evaluation were last completed, or more frequently, based on job assignment as determined by the licensee or applicant, and a

psychological re-assessment within 5 years of the date on which this element 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.

(U) The reinvestigation shall include the following:

a. **(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 statute 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). Submissions of fingerprints for the review of criminal history information should be handled separately from investigations for outage staffing to preclude inadvertent outage staffing delays.

b. **(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.

c. **(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, 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. (U) Fitness-for-Duty Considerations related to 10 CFR Section 26.10, "General Performance Objectives"

(U) The use of illegal drugs and the intentional misuse of legal drugs and alcohol are only a few of the potential causes for concern with respect to an individual's state of mind as it relates to an insider threat. In addition, physical and mental conditions that are not related to either of these may drive an individual to commit an adverse act. For example, sedative-hypnotic products (e.g., sleep disorder drugs) are widely prescribed and have been associated with adverse behavior, including aggression, sleep driving, and suicidal thoughts. Licensees should refer to NRC Information Notice 2007-31, "U.S. Food and Drug Administration Announcement Related to Certain Sleep Disorder Drugs," dated November 13, 2007, for more information. In the context of insider threat, licensees should understand the relationships between BOP relating to identifying and reporting suspicious behavior, the fitness-for-duty program relating to the evaluation of impairment-related behavior that could impact the trustworthiness and reliability of an individual, and the access authorization program that determines suitability for unescorted access.

(U) Licensees are expected to consider the potential insider threat when making fitness-for-duty determinations associated with observed abnormal behavior.

4. (U) Access to Vital Areas

(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 list must include only those individuals who have a continued need for 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. The list must be updated and reapproved no less frequently than every 31 days. The intent 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 requiring it to perform their duties.

(U) In determining continued need, licensees should consider event response, weekend or holiday emergencies, or other "off-hours" operational responses. The licensee may determine that some individuals are required to remain on the list. Personnel who fall into this category will be evaluated at the licensee's discretion. However, personnel should be evaluated by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual.

5. (U) Physical Protection Measures - Specific Elements

(U) In considering program elements needed to mitigate the AI and AVI, licensees should develop a four part program that will:

a. **(U)** ensure licensed operators are properly trained to recognize indications of tampering, which includes mis-positioning of equipment until dispositioned otherwise, to report such conditions in a timely manner, and to compensate for degraded conditions as appropriate;

b. ensure armed security officers are properly trained to recognize indications of obvious tampering;

c. ensure personnel who receive plant access training are trained in recognizing behaviors or conditions adverse to safe operations and security of the facility;

b. **(U)** develop procedures and training requirements to react effectively to conditions related to actual or suspected tampering;

c. **(U)** ensure that indications of tampering are included in the corrective action program; and (b)(7)(F)

d. [redacted]

e. The program should identify target set equipment that:

[redacted]
(b)(7)(F)

(U) While the above engineered and administrative physical protection measures relate to target set equipment, licensees should remain aware that tampering with non-target set equipment, such as safety or security equipment, can adversely affect the ability to respond to events as required in compliance with the regulations.

(b)(7)(F)

(U) Licensees should train security personnel to recognize and respond to obvious indications of tampering. Except where precluded by immediate personnel safety concerns, operations abnormalities, or restrictions under guidelines to keep radiation dose rates as low as reasonably achievable, an armed security officer should patrol accessible areas that contain target set elements.

(U) Licensee procedures should describe the operations and security response to actual tampering events. Any suspected tampering event should be entered into the licensee's corrective action program.

(b)(7)(F)

(b)(7)(F) The Nuclear Energy Institute's NEI 03-12, latest NRC endorsed revision, "Security Plan Template," describes the specifics of a patrol program that the NRC has found acceptable.

(b)(7)(F)

(b)(7)(F) 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, outlines additional guidance for these types of measures.

(OUO-SRI) Licensees should ensure that searches are performed in an acceptable manner that will ensure personnel are searched for contraband (explosives and firearms) before entering the facility. This makes contraband searches an integral physical protection element of the IMP.

D. (U) IMPLEMENTATION

(U) This section provides information to applicants and licensees regarding the NRC's plans for using this regulatory guide. No imposition or backfit is intended or approved in connection with its issuance except as discussed below.

(U) As is the case with all NRC regulatory guides, licensees are not required to implement any of the guidance described in this document. However, except in cases in which an applicant or licensee proposes or has established a method for complying with specified portions of the NRC's regulations that differs from the methods described in this regulatory guide, the NRC staff plans to use this guide to evaluate the adequacy of a licensee's IMP program.

(U) The methods described herein will be used in evaluating: (1) submittals in connection with applications for construction permits, standard plant design certifications, operating licenses, early site permits, and combined licenses; and (2) submittals from operating reactor licensees who voluntarily propose to initiate system modifications if there is a clear nexus between the proposed modifications and the subject for which guidance is provided herein.

(U) BACKFIT STATEMENT

(U) The staff prepared a backfit analysis for the final power reactor security rule for which this regulatory guide provides guidance. *See* 74 FR 13926, 13968 (March 27, 2009). This regulatory guide presents the first instance of NRC staff guidance on the amended rule. Accordingly, the backfit statement in the final 2009 power security rules applies to this regulatory guide. No further consideration of backfitting is necessary for this regulatory guide.

(U) GLOSSARY

(U) active insider— a person who, while in an unescorted access status and within the protected area, takes direct action to assist a DBT (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/or divert operations or security resources from normal protective or recovery strategies.

(U) administrative withdrawal of UAA/UA—a process to temporarily withhold UAA/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 nominal 12-month periodicity. Performance may be conducted up to three months before to three months after the scheduled date.

(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 their Commission findings.

(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 fitness-for-duty programs. Personnel are trained to report legal actions; to possess certain knowledge and abilities (K&A's) 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.

(U) 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 any individual who has been granted UA or certified UAA and performs one or more of the following job functions:

a. **(U)** any individuals who have extensive knowledge of facility defensive strategies or who design and/or implement the plant's defense strategies;

b. **(U)** any individuals in a position to grant an individual unescorted access or to certify an individual unescorted access authorization;

c. **(U)** any individuals assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices);

d. **(U)** any individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in § 73.54; and

e. any individual identified in 10 CFR 73.56(i)(1)(v)(B)(5).

(U) 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 an insider 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/UA or FFD program suitability requirements as defined in latest version of NEI 03-01 that describes an approach that the NRC staff has found acceptable.

(U) reviewing official—the licensee or, if applicable, C/V 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 and/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, and/or core disruption) barring extraordinary action by plant operators. A target

set with respect to spent fuel sabotage is 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, being subject to a BOP and training in the FFD K&A's),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) REFERENCES

(U) 1. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.[1]

(U) 2. NEI 03-01, "Nuclear Power Plant Access Authorization Program," Nuclear Energy Institute, Washington, DC.

(U) 3. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

(U) 4. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC.

(U) 5. EA-03-086, "Design-Basis Threat Order," U.S. Nuclear Regulatory Commission, Washington, DC, April 29, 2003.

(U) 6. 10 CFR Part 26, "Fitness for Duty Programs," U.S. Nuclear Regulatory Commission, Washington, DC.

(U) 7. Information Notice 2007-31, "US Food and Drug Administration Announcement Related to Certain Sleep Disorder Drugs," U.S. Nuclear Regulatory Commission, Washington, DC, November 13, 2007.[2]

(U) 8. NEI 03-12, "Security Plan Template," Nuclear Energy Institute, Washington, DC.

(U) 9. SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual," Sandia National Laboratories, Albuquerque, New Mexico, September 2007.

(U) 10. 71 FR 62664, "Power Reactor Security Requirements," *Federal Register*, Volume 71, Number 207, pp. 62664–62874, Washington, DC, October 26, 2006.[3]

Add a reference for the Proposed and Final Rules.

---

1 **(U)** All NRC regulations listed herein are available electronically through the Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/cfr/. Copies are also available for inspection or copying for a fee from 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 email PDR@nrc.gov.

2 **(U)** All information notices listed herein were published by the NRC and are available electronically through the Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/. Copies are also available for inspection or copying for a fee from 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 email PDR@nrc.gov.

3 **(U)** All *Federal Register* notices listed herein were issued by the U.S. Nuclear Regulatory Commission and are available for inspection or copying for a fee from 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@nrc.gov. Many are also available electronically through the Federal Register Main Page of the public GPOAccess Web site, which the U.S. Government Printing Office maintains at http://www.gpoaccess.gov/fr/index.html.

(U) BIBLIOGRAPHY

(OUO-SRI) PERS-TR-94-001, "Assessment of Position Factors that Increase Vulnerability to Espionage," Department of Defense Personnel Security Research Center. Provides guidance that may assist a licensee in determining which positions may be vulnerable to an insider threat based on local conditions.

(U) BIBLIOGRAPHY

(OUO-SRI) PERS-TR-94-001, "Assessment of Position Factors that Increase Vulnerability to Espionage," Department of Defense Personnel Security Research Center. Provides guidance that may assist a licensee in determining which positions may be vulnerable to an insider threat based on local conditions.

ADAMS Accession No.: ML090721034

OFFICE:	NSIR/DSP/RSRLB/TL	NSIR/DSP/RSRLB/BC	NSIR/DSP/DDRS	OGC
NAME:	BSchnetzler	DHuyck w/ comments	SMorris w/ comments	BJones Subject to edits
DATE:	03/20/09	03/24/09	03/26/09	04/14/09
OFFICE:	NSIR/DSO/	NSIR/DSP		
NAME:	BWestreich	RCorreia		
DATE:	05/30/09	06/ /09		

OFFICIAL RECORD COPY