Information For The Implementation of 420-3-26-.15 Physical Protection of Category 1 Category 2 Quantities of Radioactive Material

Information From: **NUREG-2155, Rev 1 Implementation Guidance for 10 CFR Part 37**

NUREG -2166 Physical Security Best Practices

1. The requirement to submit documents to the NRC under oath or affirmation may be satisfied by using a notary public to authenticate oaths or affirmations and to certify that the information provided is correct and true.

   I declare {or certify, verify, state} under penalty of perjury that the foregoing is true and correct, Executed on {date} {Signature}.

2. The NRC has not developed a set of criteria for determining T&R because no such list is likely to cover all licensees' needs and each licensee is in the best position to weigh the many considerations that must support such determinations. The following indicators are provided for convenience.

   Impaired performance attributable to psychological or other disorders

   Conduct that warrants referral for criminal investigation or that results in an arrest or a conviction

   Indication of deceitful or delinquent behavior

   Attempted or threatened destruction of property or life

   Suicidal tendencies or attempted suicide

   Illegal drug use or the abuse of legal drugs

   Alcohol abuse disorders

   Recurring financial irresponsibility

   Irresponsibility in the performance of assigned duties

   Inability to deal with stress or the appearance of being under unusual stress

   Failure to comply with work directives

   Hostility or aggression toward fellow workers or authority

   Uncontrolled anger, violation of safety or security procedures, or repeated absenteeism

   Significant behavioral changes, moodiness, or depression

3. Verification of true identity.

To verify the identity of an applicant for access authorization under this subsection, the employer must examine "official identification documents" to determine if they reasonably appear to be genuine and if they relate to the individual. The employer is not required to determine that the identification is authentic.

The licensee may use identity documents issued by a State or local government or by the Federal Government as long as they contain a photograph and information such as name, date of birth, gender, height, eye color, and address. These documents include passports, driver's license, and identification cards issued by Government entities.

4. Character and reputation determination.

This is similar to a reference check for employment. The following questions provide examples that the licensee should consider asking when conducting the reference check:

Would the organization rehire the individual

Would it trust the individual with company assets

Does it consider the individual to be trustworthy and reliable

Has it ever witnessed anything in the individual's behavior that would cause it to questions his or her reliability

5. What should the security plan include.

The plan must, among other things, include a description of the measures and strategies to implement the security requirements and to identify the resources, equipment, and technology used. The licensee should ensure that its security plan describes any site-specific conditions that affect how it will implement the requirements. An adequate plan requires a licensee to analyze the particular security needs of its individual facilities and to explain clearly how it will implement its chosen security measures to ensure that they work together to meet the applicable performance objectives. Recommended content is list:

A description of the radioactive material, its categorization, and its use

A description of the environment, building, and facility in which the radioactive material is used or stored and, if applicable, a diagram of the facility layout and security system

The location of the building and facility relative to areas accessible to the public

Local security procedures

Objectives of the security plan for the specific building or facility, including the following:

The specific concern that will be addressed (e.g., unauthorized removal, destruction, or malevolent use)

The kind of control necessary to prevent undesired consequences, including the auxiliary equipment that might be secured

The equipment or premises that will be secured

Security measures that will be used, including the following:

The measures to secure, provide surveillance, provide access control, detect, delay, respond, and communicate

The design features to evaluate the quality of the measures against the assumed threat

Administrative measures that will be used, include the following:

Security roles and responsibilities

Routine and non-routine operations, including an account of the source(s)

Maintenance and testing of equipment

A determination of the trustworthiness of personnel

The application of information security

Methods for access authorization

Security related aspects of the emergency plan, including event reporting

Training

Key control procedures

Procedures to address an increased threat level

The process for periodically evaluating the effectiveness of the plan and updating it accordingly

Any compensatory measures that may need to be used

References to existing regulations or standards

6. Some of the following reasons may require the licensee to revise its security plan:

A need to make changes to the physical protection program based on the results of the annual security program review

A need to increase the quantity of radioactive material that it has aggregated at a given location

A need to alter its facility in a way that could affect the security of the risk-significant radioactive material

Changes made to the measures that it relies upon to comply with 10 CFR Part 37

7. The following are examples for security plan training:

The controls that are in place to prevent unauthorized access to material

The purpose and functional requirements of the licensee's alarm and access control systems

Notification procedures in the event of an unauthorized access for potential malevolent activities

Ways to confirm quickly and accurately whether an intrusion is likely to be intentional or accidental

8. The licensee shall conduct refresher training on the security plan. The refresher training should address the following items:

Any changes to the security program since the last training

Any changes in the assigned responsibilities of individual trainees that would require new training

Recent information on any relevant security issues or lessons learned

Relevant results from the program review or any NRC inspections

Relevant operating experience form the maintenance and testing program for security systems or system components

9. The following goals are necessary to design a protection-in-depth strategy for the physical protection program:

Increase the adversary's uncertainty about the physical protection program

Require the adversary to more extensively prepare before he or she attacks the facility

Create additional steps that may cause the adversary to fail or abort the mission

10. The principle of a balanced design requires the strengthening of doors, windows, or other openings and their associated frames, hinges, bolts, and locks to afford the same amount of delay as that provided by the floors, walls, and ceilings of the structure. The licensee should consider the following protective measures for doors, windows, and other openings:

Limit the number of doors, windows, and other openings for the room/structure in which the facility uses or stores the risk-significant radioactive material

An adversary cannot lock door locks if the door-locking hardware/keyways are not exposed. For doors that do not need to be used as an entrance (only for exit), the licensee should consider removing external hardware and covering all external holes if safety and/or fire code requirements allow such measures (e.g., door opening hardware that is inside the room cannot be compromised from outside)

For standard doors, adding steel plates to the surface of the door, using security door hinges that have a stud-in-hole feature, and grouting the door frame with concrete will strengthen the supporting structure of the door and will increase penetration time

Wood cores, especially redwood, placed between door plates increases the penetration time for thermal cutting tools by a factor of 3 to 4 times that of a hollow door

To help prevent an adversary from prying open the door at the separation between the door lock and door frame, a strip of sheet steel can be welded or bolted to the door. This strip should be the same height as that of the door and should be at least 2 inches wide with a 1-inch overlap onto the adjacent door frame

Replacing a standard door lock with a high-security lock with a multiple deadbolt system or using door-intrusion sensors, or both, will mitigate lock vulnerabilities

For windows, the licensee should use glass glazing materials, such as laminate, Lexan or wire glass that is specifically meant for security applications (e.g., not just safety glass). For the window frame, the licensee should use additional or heavier fasteners or should consider welding the frame in place

A window that can open should have substantial fastening devices or should be replaced with a fixed window (i.e., a window that cannot be opened) if safety and fire code requirements allow such measures

For other openings (e.g., utility ports) and windows, the licensee should use metal grates, grills, steel bars, and expanded metal mesh and should consider reducing the size (e.g., dimensions less than 6 inches) of the opening to prevent the ability to crawl through the opening

11. The licensee should consider the following items when using key, combination, cipher, or electric locks:

The licensee should select locks specifically designed for security applications, not common builder's hardware-type locks found in home improvement stores

For key locks, the lock should be capable of being set for a large number of different keys. (For example, the licensee should have enough keys for the number of people who will need access to the lock and should have extra keys for keys that are lost or for the turnover of personnel)

The licensee should ensure that the key cut required to open a lock is changeable so that a key can no longer be used when keys are lost or when an employee who has access to a key no longer requires access

A master-keyed locking system (i.e., using multiple locks that have one master key should not be used for locks located within the security zone

Padlocks used to secure external barriers should be of rugged and sturdy construction and designed for outdoor use

If combination locks or padlocks are used, the licensee should use locks that meet Federal Specification FF-P-110J(1), "Padlock, Changeable Combination Lock (Resistant To Opening by Manipulation and Surreptitious Attack)," dated February 11, 1997

For controlling access, electric locks or electronic cipher locks are preferred because the exposed part of the lock is isolated from the part that contains the code, they offer versatility in programming (e.g., fairly easy change to combination/access permissions), and they can be integrated into the alarm system (e.g., ability to prevent trial and error methods of surreptitious attack an alarm after a number of unsuccessful attempts)

The licensee should protect electric locks against tampering by using tamper switches that are connected to the alarm system

12. The licensee should consider the following factors when installing locks:

The lock should be placed as far as it can from the face of the door, or a guard plate should be used that covers as much of the lock's cylinder as possible (while still permitting the key to be turned)

Special security screws should be used to mount security hardware located outside the secured area. The security screws should require a special tool for their removal, or they should not be able to be removed once they are installed (e.g., heads welded to the hardware/device)

Screws that are used to mount a security device should also be hardened

If the lock or fastening hardware is mounted on wood, the licensee may achieve a higher level of protection by using screws that are long and strong enough to be embedded in the underlying structure (e.g., screws into wood framing or a concrete wall, or both)

13. Many types of credentials can be used as part of the identity verification system. Coded credential systems have a wide range of capabilities and can do the following:

Eliminate the need for a manual check because the appropriate card reader system can automatically check an individual's authenticity

Assign a unique identification code number to the credential that can be read by a machine

Maintain entry authorization records for each coded credential

Terminate access authorization for an individual without the necessity to recover the individual's credential (e.g., key card)

Assign different levels of access authorization, such as assigning access authorization to specific (i.e., not all) access control points or providing access only at certain times of the day

14. Licensees must develop, maintain, and implement written policies and procedures to ensure that only trustworthy and reliable individuals with a need to know are allowed access to security plans and procedures. The licensee's policies and procedures should do the following:

Include a general performance requirement that each person who produces, receives, or acquires the licensee's sensitive information ensures that such information is protected against unauthorized disclosure

Address how to protect sensitive information while in use, storage, and transit

Address the preparation, identification or marking, and transmission of documents or correspondence containing the licensee's security program information

Address how access to the licensee's security program information is to be controlled

Include methods for the destruction of documents that contain security program information

Include procedures for the use of automatic data processing systems that contain security program information

Address the removal of documents from the licensee's protected information category when they become obsolete or no longer sensitive

15. Coordination with LLEA and information that a licensee could discuss includes, but not limited to, the following:

Types and quantities of devices and radioactive material possessed

Potential hazards associated with loss of control of the devices and radioactive material

Specific facility information (i.e., contact information, floor plans, entrances, points of egress, or other information)

Site-specific physical protection measures that the licensee employs to delay an adversary from gaining access to the radioactive material

Established protocol for contacting the LLEA in response to an event

Licensee and LLEA points of contact for plans to recover stolen material that has been removed to an offsite location

16. For an effective response, the following actions should be taken:

Provide the LLEA with sufficient detailed information about the facility or site and provide a description of the risk-significant radioactive material and the potential hazards

Provide the LLEA with updates of information about the facility, the risk-significant radioactive material, or the storage and use of the material changes

Ensure that reliable and redundant communications are always available (e.g., two-way radios and landline telephones

Conduct response training and exercises periodically to validate and improve response force readiness

Conduct periodic face to face meetings with the LLEA

Perform periodic testing of the alarm response with the LLEA

17. The administrative security measures should include the following key subject areas:

Authorization requirements for access to risk-significant radioactive material and sensitive information

A determination of the trustworthiness and reliability of individuals who require unescorted access to risk-significant radioactive materials (i.e., category 1 and category 2 quantities of radioactive material)

Security training requirements for individuals responsible for security

Procedures for protective the risk-significant radioactive materials and sensitive information (e.g., security plan)

Maintenance and testing of security equipment (e.g., detection sensors, alarms, and video assessment equipment

Compensatory security measures that address security equipment failures or emergencies, or both, without degrading the physical protection program

Response planning and coordination

18. Maintenance and testing must be performed at the manufacturer's suggested frequency or at least annually if the manufacturer has no suggested frequency. What minimum measures should a licensee implement for maintenance and testing program. A licensee should do the following:

Identify all alarms, communication systems, and other physical components necessary to secure radioactive materials or to detect unauthorized access to them

Specify the intended function of each component identified in the program and the minimum performance required to fulfill that function

Specify the test(s) that it will conduct on each component and identify the minimum quantitative or qualitative test results that are required for finding the component operable and capable of performing its intended function

Identify the testing equipment that it will use and prescribe any device-specific procedures necessary for the used or maintenance of this equipment

Identify the measures that it will apply to ensure that the testing equipment used in the program will perform in service as expected

Prescribe procedures for the routine maintenance of each intrusion alarm, communications system, and physical component of both the system used to secure the subject radioactive material and the system used to detect unauthorized access

Require a written record for each and maintenance activity performed on the security or detection system

19. The licensee shall maintain records on the maintenance and testing activities for 3 years. For each maintenance activity, a record should identify the follow items:

The name(s) of the person(s) who performed the maintenance

The date that the maintenance was performed

The component(s) or system(s) on which the maintenance was performed

The purpose of the maintenance, identifying, as appropriate, the deficiencies in operability of performance

Any maintenance activities needed to remove any deficiency in the operability or performance of the component or system

20. For each activity, a record should identify the following items:

The name(s) of the person(s) who performed the testing

The date of the testing

The component(s) or system(s) tested

The purpose of the testing

The performance expected to fulfill the component's or system's intended function

The results of the testing

Any maintenance activities needed to remove any deficiency in the operability or performance of the component or system

21. Contingency planning is an important part of ensuring the security and accountability of the risk-significant radioactive materials in the event of an emergency situation or an unexpected event that could affect the security of the risk-significant radioactive material. The following examples are some events that the licensee should consider:

An unexpected evacuation (e.g, bomb threat or fire)

Serious natural events that have an increased probability of occurring in the area in which the facility or site is located (e.g, floods, earthquake, and tornado)

Damage or destruction of the facility or security zone, or both, which may require the need to move or recover the risk-significant radioactive material

Loss of power, including backup power

Loss of all outside communications (e.g., radio, cell phone, and landline) or an inability to contact the response force

22. The shipping licensee must investigate immediately if a category 1 shipment is lost or missing or if a category 2 quantity shipment does not arrive by the No-Later-Than-Arrival-Time. The investigation should include:

Determine the time and location of the last transport crew check-in

Determine where communication was lost

Determine where tracking was lost

Confirm that the equipment is working properly

Contact the escort if one was being used

23. The administrative process for access control should include the following key aspects:

Issuance, control, and accounting of access media and codes (e.g., keys, identification cards, lock combinations, personal identification numbers, and alarm system codes

Requirements for access rights to controlled areas

Termination of access rights when access is no longer needed

Visitor management and escort procedures

A change in keys, combinations, alarm system codes/passwords, and other access media when they are lost or compromised

Operation and management of electronic access control system (if applicable)

24. The detection system of an effective physical protection program should include the following attributes:

The system has redundant critical elements (e.g., use of a balanced magnetic sensor and infrared motion sensor for the same room

The system has complementary technologies so that the adversary has to use a variety of defeat methods (e.g., use passive infrared motion sensor and an active microwave motion sensor to detect the same area)

The system has low nuisance and false alarm rates and has a high probability of detection

The system can detect tampering (e.g., loss of interruption in the alarm signal line)

The system is reliable and robust for the type of operating environment (e.g., an outside or inside environment or an arctic or hot climate)

The system is combined with a good assessment system (Note that the detection function is not completed without assessing what was detected)

The system is regularly maintained and tested through a performance testing program