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

December 2014
Division 5

DRAFT REGULATORY GUIDE

Technical Lead
Al Tardiff

DRAFT REGULATORY GUIDE DG–5027

(Proposed Revision 1 of Regulatory Guide 5.12, dated November 1973)

GENERAL USE OF LOCKS IN PROTECTION AND CONTROL OF FACILITIES AND SPECIAL NUCLEAR MATERIALS, CLASSIFIED MATTER, AND SAFEGUARDS INFORMATION

A. INTRODUCTION

2740
Purpose

This regulatory guide describes methods and procedures that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for the selection, use, and control of locking devices in the protection of areas, facilities, and specific types of information (e.g. classified matter, National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD), Safeguards Information (SGI), and Special Nuclear Material (SNM)).

Applicable Rules and Regulations

- Title 10, Part 50, of the *Code of Federal Regulations* (10 CFR Part 50) (Ref. 1), "Domestic Licensing of Production and Utilization Facilities," specifically 50.34(c) "Physical Security Plan," requires that each applicant for an operating license for a utilization facility must submit a physical security plan.

- Title 10, Part 70, of the *Code of Federal Regulations* (10 CFR Part 70), "Domestic Licensing of Special Nuclear Material," (Ref. 2), specifically 10 CFR 70.22(h), "Contents of applications," requires that certain licensees submit an NRC-approved physical security plan.

- Title 10, Part 73, of the *Code of Federal Regulations* (10 CFR Part 73), "Physical Protection of Plants and Materials," (Ref. 3), specifically 10 CFR 73.40, "Physical protection: General requirements at fixed sites," requires that certain licensees provide physical protection at a fixed site, or contiguous sites where licensed activities are conducted, against radiological sabotage, or against theft of SNM, or against both.

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received final staff review or approval and does not represent an official NRC final staff position. Public comments are being solicited on this draft guide and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal–rulemaking Web site, http://www.regulations.gov, by searching for Docket ID**:** NRC-2014-0276>. Alternatively, comments may be submitted to the Rules, Announcements, and Directives Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this draft regulatory guide, previous versions of this guide, and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at http://www.nrc.gov/reading-rm/doc-collections/reg-guides/. The draft regulatory guide is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML14002A224. The regulatory analysis may be found in ADAMS under Accession No. ML14002A222

- Title 10, Part 73, "Physical Protection of Plants and Materials," specifically 10 CFR 73.22(c)(2), "Protection of Safeguards Information: Specific Requirements," requires that SGI be stored in a locked security storage container when unattended.

- Title 10, Part 34, of the *Code of Federal Regulations* (10 CFR Part 34), "Licenses for Industrial Radiography and Radiation Safety Requirements for Industrial Radiographic Operations," (Ref. 4), specifically 10 CFR 34.23(a) and (b), "Locking of radiographic exposure devices, storage containers and source changers," requires locking of radiographic exposure devices, storage containers and source changers.

- Title 10, Part 35, of the *Code of Federal Regulations* (10 CFR Part 35), "Medical Use of Byproduct Material," (Ref. 5), specifically 10 CFR 35.615, "Safety precautions for remote afterloader units, teletherapy units, and gamma stereotactic radiosurgery units," describes requirements that pertain to a licensee having an electrical interlock system for each entrance to a treatment room.

- Title 10, Part 36, of the *Code of Federal Regulations* (10 CFR Part 36), "Licenses and Radiation Safety Requirements for Irradiators," (Ref. 6), specifically 10 CFR 36.23, "Access Control," 10 CFR 36.31, "Control of source movement," 10 CFR 36.37, "Power failures," 10 CFR 36.39, "Design requirements," 10 CFR 36.41, "Construction monitoring and acceptance testing," and 10 CFR 36.67, "Entering and leaving the radiation room," describe requirements for a licensee to implement specific locking conditions.

- Title 10, Part 37, of the *Code of Federal Regulations* (10 CFR Part 37), "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material," (Ref. 7), provides the requirements for the physical protection program for any licensee that possesses an aggregated category 1 or category 2 quantity of radioactive material listed in Appendix A to 10 CFR Part 37.

- Title 10, Part 39, of the Code of Federal Regulations (10 CFR Part 39), "Licenses and Radiation Safety Requirements for Well Logging," (Ref. 8), specifically 10 CFR 39.31(b), "Security precautions during storage and transportation," 10 CFR 39.63, "Operating and emergency procedures," and 10 CFR 39.71, "Security," describe licensee requirements to have locks in place.

- Title 10, Part 95, of the *Code of Federal Regulations* (10 CFR Part 95), "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," (Ref. 9), specifically 10 CFR 95.25(a) and (j), "Protection of National Security Information and Restricted Data in storage," and 10 CFR 95.29, "Establishment of Restricted or Closed areas," describe licensee requirements to provide locks for the protection of classified matter and information.

Purpose of Regulatory Guides

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

This regulatory guide contains information collection requirements covered by:

- 10 CFR Part 50 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0011,
- 10 CFR Part 70 that OMB approved under OMB control number 3150-0009,
- 10 CFR Part 73 that OMB approved under OMB control number 3150-0002,
- 10 CFR Part 34 that OMB approved under OMB control number 3150-0007,
- 10 CFR Part 35 that OMB approved under OMB control number 3150-0010,
- 10 CFR Part 36 that OMB approved under OMB control number 3150-0120,
- 10 CFR Part 37 that OMB approved under OMB control number 3150-0214,
- 10 CFR Part 39 that OMB approved under OMB control number 3150-0120,
- 10 CFR Part 95 that OMB approved under OMB control number 3150-0047.

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. DISCUSSION

Reason for Revision

Revision 1 of RG 5.12 incorporates new information, lessons learned, and operating experience since the guide was originally issued in 1973, particularly new locking technologies and standards for locks and keys. In addition, the guide contains updated references and relevant regulations were identified.

Background

Locks are essential components of a physical barrier that can be used to meet the physical protection requirements identified. Locks assist in controlling access to areas, facilities, materials and information through doors, gates, containers, and similar materials or personnel access controls. NUREG-1964, "Access Control Systems," (Ref. 10), discusses information related to designing, installing, testing, maintaining, and monitoring access control systems used for the protection of facilities licensed by the NRC.

A lock is a mechanical latching device for securing moveable portions of physical barriers (e.g., doors, gates, drawers) in a secured position. Locks are very important components of a physical barrier, but they should be considered as delay devices only, rather than permanent impediments to unauthorized entry, since any lock can be defeated by expert manipulation or force given enough time.

Ideally, the lock delay capability should match the penetration resistance of the rest of the barrier. The effectiveness of locks, however, lies in their use in conjunction with other security measures that balance the protection afforded across multiple surfaces and points of entry, since a potential adversary seeks to minimize the time or detection inherent in the defeat or bypass of a given security layer. To this end, multiple barrier systems, seals, tamper safe devices, intrusion detection and alarm systems, and response actions should be considered as an integrated system. This integration should include evaluation of the door or barrier materials, hinges, frame, and nearby wall and mounting surfaces to identify weaknesses that could enable an adversary to bypass the locking system in favor of a more advantageous pathway.

Locks are commonly categorized by the mechanism used to withdraw the latching system to allow access. The most common mechanisms are by entry of a specific sequence of numbers in the case of combination locks, manipulation with a key in the case of keyed locks, and presentation of electronic security tokens in the case of electronic locks. Locks and locking systems can further be categorized as being part of entry control or access control systems. Lock componentry, as described in this regulatory guide, are elements of entry controls. Components of locks generally consist of a mechanical latching device for securing a movable portion of a security barrier, and include items such as keys, combinations, and physical latching systems. Access control systems, as described in NUREG-1964, are identity verification and search procedures and equipment. The components of access control could include procedures, contraband detection, computers, electronic databases, and associated detection, alarm, and communications infrastructure.

This guide uses a number of technical terms and phrases related to lock systems. Definitions and explanation of these lock terms can be found in "The Professional Locksmith Dictionary." (Ref. 11)

Combination Locks

In a combination lock, the locking mechanism is disengaged by entering a specific sequence of numbers (i.e., the combination). A combination lock should be designed to provide a large number of possible combinations. The number of possible combinations is determined by the number of numerals available for each number in the sequence and the length of the sequence. For example, a lock having 100 possible numerals (i.e, 0 through 99) and a three-number sequence (e.g., "0-10-30") offers 1 million (100 x 100 x 100) combinations. Some combination locks require a four-number sequence (e.g., "0-10-30-40").

Combination locks are designed for use in two basic forms. The first is a case lock, in which a combination lock is mounted on or into a door or container as a mortise or rim lock, and the second is a padlock. High-quality combination locks are tested for resistance to surreptitious entry (e.g., manipulation, radiological analysis, and emanations analysis) and forcible entry.

Protection against forcible attack on a mortise or rim-mounted lock can be increased if the lock is equipped with hardened steel plates and if it is designed with relocking triggers or devices that dead lock the bolt or bolt-actuating mechanism upon forcible attack. These locks should use a deadbolt and not a dead-locking latch, which is more susceptible to force. The deadbolt should have a minimum 1-inch lateral throw or multiple vertical engagements with its strike. Astragals (i.e., the vertical member attached to the meeting edge of one door panel of a pair, bridging the opening and holding one door panel inactive) on outswinging doors and inswinging double doors without mullions (i.e., the stationary member of the frame used to separate door panels) provide additional protection to the lock bolt.

Security can be increased by frequently changing a lock's combination; hence, locks in which the combination can be readily changed are desirable. Some locks permit a new combination to be directly

entered when using a special key inserted into the back of the lock. These locks are commonly termed "key-change" locks. Others require the replacement of internal parts to change the combination.

Combination locks may be vulnerable to compromise if the back of the lock is readily available (e.g., when the back of the lock is accessible or the lockable access is open). Removing the back cover from the lock may allow the combination to be determined. The combinations of some key-change locks can be changed directly when the lock is in the open position, while others must have the existing combination reentered to a different index when the access is in the open position to permit the combination change. The former type permits an intruder to quickly change the combination to one of his or her own choosing. This would allow an intruder entrance after the lock is closed, but deny entry to an authorized user. For these reasons, backplates or other devices should be used to protect the back of the lock, and the door or container in which the lock is located should not be left unattended when open.

In a mechanical pushbutton lock, the pushbuttons activate linkages that connect a gate with an external knob to permit opening of the lock. This type of lock typically offers relatively few possible combinations, and therefore can be defeated by simply attempting each possible combination until the correct combination is discovered. Infrequent combination changes can lead to wear patterns on the pushbuttons, which can further reduce the number of combinations an intruder would need to enter to gain unauthorized entry. For electronic locks (e.g., keypads), a limited set of possible combinations can be balanced by limiting the number of unsuccessful attempts to access the lock (e.g., after ten failed attempts the lock would refuse to open even for the correct combination). However, it is difficult to limit the number of unsuccessful attempts for mechanical pushbutton locks.

Federal Specification FF-L-2740, "Locks, Combination," (Ref. 11) covers changeable combination locks designed to be mounted on safes, security files, vault doors, and similar items that are intended for the protection of classified matter. To be approved by the U.S. General Services Administration (GSA), security file cabinets, map and plan containers, vault doors, and doors for facilities approved for open storage of classified information must be secured with a lock that has been tested and approved under Federal Specification FF-L-2740. The only exception is for field safes (safes specifically designed and built for the protection and storage of classified material in other than fixed facilities), which may use a lock meeting the standards in Underwriters Laboratories (UL) 768, "Standard for Combination Locks," (Ref. 12) Group 1R.

Figure 1. Field safe

Locks meeting Federal Specification FF-L-2740 resist 20 man-hours of manipulation, 20 man-hours of radiological analysis, 20 man-hours of emanations analysis, and 30 man-minutes of covert opening. Three locks have been approved under Federal Specification FF-L-2740—models X-07, X-08, and X-09. All three models are self-powered electromechanical locks. While all three models are still approved, only the X-09 is currently being produced.

Figure 2. X-09 lock

Pedestrian door deadbolts covered by Federal Specification FF-L-2890, "Lock Extension (Pedestrian Door, Deadbolt)," (Ref. 13) are intended for use on interior pedestrian doors into areas of facilities approved for open storage of classified information. This specification is intended for deadbolts located on interior pedestrian doors used for normal entrance and egress during day-to-day operations. A pedestrian door deadbolt meeting Federal Specification FF-L-2890 consists of a mounting plate, a combination lock that meets Federal Specification FF-L-2740, and a strikeplate. The mounting plate is surface mounted to the inside face of the door. The deadbolt baseplate has two essential features. First, it provides a means of latching the bolt in the retracted position. This prevents the bolt from being inadvertently extended. Second, turning a knob on the baseplate will retract the bolt to allow egress. Proper deadbolt operation requires installation of the correct strikeplate. The strikeplate needed depends on the door bevel and whether it is a single- or double-door leaf. Pedestrian door locks meeting the requirements of Federal Specification FF-L-2890 that feature single-motion egress for life safety is available and applicable for protection of facilities approved for open storage of classified information. These locks can be mated with a variety of access control devices.

New and existing GSA-approved weapons containers and armory vault doors for the protection of arms, ammunition, and explosives require locks that meet the requirements of UL 768, Group 1. Effective March 1, 2008, all GSA-approved weapons containers and armory vault doors, will be manufactured with a lock that meets Federal Specification FF-L-2937, "Combination Lock Mechanical," (Ref. 14) Group 1 locks resist manipulation attempts for 20 man-hours. In addition to this protection, these locks all have protection against a common method of forced entry. They have internal relock triggers that prevent retraction of the bolt if the dial is removed and the spindle is punched. Combination locks that meet the requirements of FF-L-2740 should not be used on weapons (i.e., firearms) containers and armory doors.

Federal Specification FF-L-2937 is a relatively new specification. The requirements of Federal Specification FF-L-2937 correspond to the requirements of UL 768, Group 1. GSA-approved weapons containers and armory vault doors will use locks approved under Federal Specification FF-L-2937 effective March 1, 2008.

Federal Specification FF-P-110, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)," (Ref. 15) covers changeable combination padlocks designed to conform to the standards for security equipment set forth in the "Classified National Security Information Directive No. 1" (Ref. 16). These padlocks are required to resist opening for not less than 30 man-minutes by manipulation and 10 man-minutes by surreptitious attack, but are not tested for forced opening. These padlocks are intended for use onshore and aboard ocean-going vessels, indoors, or outdoors (in areas that are semiprotected by a structural overhang similar to eaves or a lean-to).

The standards in American National Standards Institute/Builders Hardware Manufacturers Association (ANSI/BHMA) A156.5-2001, "American National Standard for Auxiliary Locks and Associated Products," (Ref. 17) provide current guidance for mechanical pushbutton locks.

Key Locks

Most keyed locks fall into four general classes—warded locks, wafer (or disk) locks, lever locks, and pin-tumbler locks. In the United States, the most common type of keyed lock for security purposes is the pin-tumbler.

As in the case of combination locks, a key lock should be capable of being set for a large number of different keys (i.e., it should be difficult to guess the correct key shape to open the lock). Compare a handcuff key to an ordinary house key. A high-quality six-pin lock with 10 key cutting levels per pin potentially permits 1 million different keys to be used. However, this large a number of key cuts is not as useful as a large number of combinations because less time-consuming techniques for defeating key locks are available. Beyond basic pin-tumbler locks, several high-security lock cylinders are available. These provide considerably increased resistance to covert and surreptitious attack. They also offer greater key control capability because key blanks (e.g., the shape of the grooves a key needs on the side to be able to insert into the lock) may not be available commercially.

Licensees choosing to use master keying and interchangeable core systems should be aware of the susceptibilities created by such systems. Master keying should be done correctly to minimize the loss of security associated with such as system. Master-keyed systems and interchangeable core systems (which require a control key) should be set up so that distinct areas/programs are not under the same master key or control key. Likewise, highly sensitive areas and areas containing sensitive information should not be master keyed at all. Furthermore, where interchangeable core locks are not routinely monitored (e.g., a padlock on the gate at a remote site), the control key should be unique to that padlock. Control keys should only be issued to the individual in charge of the lock program.

Master keying is undesirable from a security point of view because disassembly and inspection of any lock in the system by a competent person provides access to all the other locks in a master-keyed system. Master keying is prohibited for the protection of classified information or matter per 10 CFR 95.25(j). In addition, termination of an employee who had access to a master key would require changing the bitting of all locks set for the master key. Changing the bitting of a large number of locks can be costly, but the convenience of master systems is such that there is strong pressure to use them. A compromise in this conflict between convenience and security may be to use a nonmastered set of locks for protected areas, material access areas, vital areas, access to vital equipment, and areas containing NSI, RD, and SGI, and to permit master key sets for other, less sensitive areas.

It is essential for a bolt of a lock to be retained in the locked position by positive means (i.e., it should not be possible to move the bolt without opening the lock) (dead bolt). In some locks, the bolt is held in a locked position by a spring only. This permits, in the case of padlocks, the use of appropriate rapping or shimming techniques; and, in the case of door locks, the opportunity to surreptitiously retract the bolt without the use of force.

The pneumatic deadbolt locking system (PDLS) was designed by the U.S. Army and has acceptable forced entry protection. The PDLS is in compliance with Military Specification MIL-DTL-43607, "Padlock, Key Operated, High Security, Shrouded Shackle," (Ref. 18). The PDLS typical configuration has six hardened steel bolts and the locking system behind the door panel. The steel bolts extend from brackets, located behind and on the door panel, into the surrounding structure.

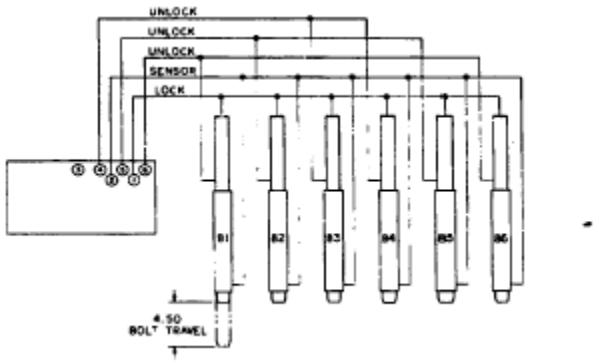

Figure 3. Pneumatic Deadbolt Locking System

UL 437, "Key Locks," (Ref. 19) covers door locks and locking cylinders, as well as other types of locks. It provides for testing in terms of security, endurance (cycle test), and salt fog test. A salt fog test provides a controlled corrosive environment that has been used to produce relative corrosion resistance information for specimens of metals and coated metals. Salt fog testing is described in ASTM International B-117-07a, "Standard Practice for Operating Salt Spray (Fog) Apparatus," (Ref. 20).

American Society for Testing and Materials (ASTM) F883, "Standard Performance Specification for Padlocks," (Ref. 21) covers key-operated padlocks and has provisions for graded testing in terms of security, endurance (cycle test), and environmental attack.

Federal Specification FF-P-2827, "Padlock, Key Operated, General Field Service," (Ref. 12) covers key-operated padlocks intended for outdoor use. These padlocks are tested to the highest levels of environmental attack in ASTM F883 and provide moderate resistance to forced entry and picking.

Military Specification MIL-DTL-43607, "Padlock, Key Operated, High Security, Shrouded Shackle," covers high-security, shrouded shackle padlocks intended for protection of military arms, ammunition, and explosives. These padlocks are intended to be used as a system with a high-security shrouded hasp that meets the requirements of Military Specification MIL-DTL-29181, "Hasp, High Security, Shrouded, for High and Medium Security Padlock," (Ref. 23).

The Internal Locking Device (ILD), designed by the U.S. Navy, is a keyed lock that provides acceptable forced entry protection. In the ILD, the locking system is located behind the door panel or in a protected housing. The Navy-designed ILD, in addition to possessing increased resistance to forced entry, is resistant to surreptitious neutralization attempts by picking, shimming, impressioning, and bypassing methods. These qualifications are the same as the U.S. Department of Defense's (DoD's) high security padlock and meet Military Specification MIL-DTL-43607. The DoD has approved the Navy-designed ILD lock for protection of conventional arms, ammunition, explosives, nuclear weapons, and chemical weapons.

Figure 4. Internal locking device

Electronic Locks

An electronic lock is a system comprised of an automatic door closer on the door, an input device, a controlling device, and a lock, usually mechanical, which is released or activated when the correct combination is entered or correct token is presented. Various technologies are available in such systems, including biometric, magnetic-stripe cards with a unique identifier encoded onto the card, proximity cards containing a unique identification code in a microchip that transmits when the card is near a card reader, smart cards that contain a memory chip to store identification data, and combination entry. A good system will use two or more of these methods. For example, an employee's photo identification card can also serve as a smart card that awakens a digital scramble keypad into which the employee enters a personal identification number. A scramble keypad places the keys on the keypad in a random order which facilities protection against an observer perceiving the number sequence being applied. A system using two technologies is referred to as a two-factor authentication system. The electronic lock offers a number of advantages, including isolation of the lock part containing the code from the exposed part of the lock, versatility of programming, and ease of integration into alarm systems.

In the event of a power failure, an electronic lock system should "fail secure." That is, doors should remain locked to personnel on the unprotected side, but egress from the secure side should remain possible. The mechanical lock is often a case lock in the door. There is often a physical key to its cylinder, the emergency override key, that can be used to gain access to areas during a power outage. Only authorized personnel should have that key.

The actual unlocking and locking of the door often is accomplished by use of an electric strike. This is mounted in the frame, and the lock's bolt projects into it. It is released when electric current is sent to it, based on a valid opening (e.g., insertion of the correct card). The electric strike should be selected depending on the amount of use it will get, and it should be periodically checked to see that it holds the door locked when it should.

If the system involves a person pressing buttons or switches to enter a code, a sight barrier should be present to prevent observation of the code as it is entered. A system in which each person presents a unique credential (e.g., an ID with electronic chip) or enters a unique personal identification number is much better than one that uses a single combination. In the former system, if an employee were to retire or be debriefed from the program, that employee's access can be removed from the system without affecting the other employees. In the latter system, all employees with access to the area would need to be given the new combination.

Pushbutton systems should incorporate devices or programming that prevent trial and error methods of surreptitious attack by activating an alarm after a certain number of unsuccessful attempts or by introducing a delay after each unsuccessful attempt, which prevents operation of the lock for a period of time.

Current guidance and specifications for electric locks include UL 1034, "Burglary-Resistant Electric Locking Mechanisms," (Ref. 24) and ANSI/BHMA A156.25-2003, "American National Standard for Electrified Locking Devices," (Ref.-25).

Control of Locks, Keys, Key Cards, Combinations, and Related Equipment

Possession of keys, key cards, combinations, and other related equipment by unauthorized individuals severely affects security and neutralizes the primary purpose of an access control program. Additionally, information gained from spare locks and related equipment can allow unauthorized individuals to gain access. For this reason, distribution of keys, key cards, combinations, and other items allowing access and storage of spare locks and related equipment should be carefully controlled.

Licensees should develop, implement, and maintain a formal process for distributing locks, keys, key cards, combinations, and related equipment to only authorized personnel; accounting for spare components; and changing keys, key card processing systems, and combinations when an individual's authorization for access has been revoked or suspended for whatever reason.

Harmonization with International Standards

The International Atomic Energy Agency (IAEA) has established a compendium of publications which address the security-related recommendations to prevent, detect, and respond to theft, sabotage, unauthorized access or other malicious acts involving nuclear material and other radioactive substances in facilities and during transport. Pertinent to this regulatory guide, IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/22/Revision 5)" (Ref.26), addresses the recommended elements of a State's physical protection regime's use, storage, and transport of nuclear materials. This regulatory guide incorporates similar design and operational guidance and is consistent with the principles provided in Nuclear Security Series No. 13.

Documents Discussed in Staff Regulatory Guidance

This regulatory guide endorses the use of one or more codes or standards developed by external organizations, and other third party guidance documents. These codes, standards and third party guidance documents may contain references to other codes, standards or third party guidance documents ("secondary references"). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in a regulatory guide as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific regulatory guide. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a regulatory guide, then the secondary reference is neither a legally-binding requirement nor a "generic" NRC approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

1. Selection and Use of Locks To Protect NSI, RD, and FRD

Regulations in 10 CFR Part 95 establish requirements for safeguarding Secret and Confidential NSI, RD, and FRD received or developed in conjunction with activities licensed, certified, or regulated by the Commission.

Regulations in 10 CFR Part 95.25(a) require the protection of NSI and RD when in storage. The material must be stored in a safe, steel file cabinet, safe-type steel file container that has an automatic unit locking mechanism, or steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets, or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key-operated or combination padlock.

Regulations in 10 CFR Part 95.29(c)(3) require that entrances and exits to restricted or closed areas must be secured by either an approved built in combination lock or an approved combination or key operated padlock.

a. Combination locks on classified storage containers (GSA approved security containers) should meet Federal Specification FF-L-2740 or UL 768 Group 1 or Group 1R specifications for locks. Existing classified storage containers, that have a UL 768 Group 1 or Group 1R specification lock that needs replacement, should be outfitted with a lock that meets Federal Specification FF-L-2740. When new classified storage containers are anticipated to be purchased they should be procured with a lock that meets Federal Specification FF-L-2740.

b. Combination locks installed in doors inside of, or leading to, areas containing classified matter should meet Federal Specification FF-L-2740 (if in vault doors) or should be pedestrian door deadbolts meeting Federal Specification FF-L-2890 (for doors to vault-type rooms).

c. Combination padlocks, rather than key padlocks, should be used when practical. Combination padlocks should be three-position, dial-type changeable-combination padlocks that meet Federal Specification FF-P-110.

d. When combination locks are used, the requirements of 10 CFR Part 95.25 sections (c), (d), (e), and (f) apply.

e. When key-operated padlocks are used, the requirements of 10 CFR Part 95.25(j) apply.

2. Selection and Use of Locks To Protect SGI

Regulations in 10 CFR Part 73.22(c)(2) require SGI to be stored in a locked security storage container when unattended.

Secure storage containers, as defined in 10 CFR Part 73.2, “Definitions,” include steel filing cabinets equipped with a steel locking bar and a three position, changeable combination, GSA-approved padlock and security filing cabinets that bears a Test Certification label on the side of the locking drawer, or interior plate, and is marked, “General Services Administration Approved Security Container” on the exterior of the top drawer or door.

Regulations in 10 CFR Part 73.22(c)(2) further require that knowledge of lock combinations protecting SGI must be limited to a minimum number of personnel for operating purposes who have a ''need to know'' and are otherwise authorized to access SGI in accordance with the provisions of this Part. Access to lock combinations should be strictly controlled to prevent disclosure to an individual not authorized to access SGI.

a. Combination locks installed in doors in, or leading to, areas containing SGI should meet Federal Specification FF-L-2740 (if in vault doors) or should be pedestrian door deadbolts meeting Federal Specification FF-L-2890 (for doors to vault-type rooms).

b. Combination padlocks should be three-position, dial-type changeable-combination padlocks meeting Federal Specification FF-P-110.

3. Selection and Use of Locks to Protect Facilities and SNM under Part 73

Under 10 CFR Part 73.55(e)(4), consistent with the stated function to be performed, openings in any barrier or barrier system established to meet the requirements of 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," must be secured and monitored to prevent exploitation of the opening. Locks are essential components of a physical barrier and assist in controlling access to areas, facilities, and materials through doors, gates, container lids, and similar material or personnel access.

Regulations in 10 CFR Part 73.51(d)(7) require a personnel identification system and a controlled lock system be established and maintained to limit access to spent nuclear fuel and high level radioactive waste to only authorized individuals.

Regulations in 10 CFR Part 73.67, "Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance," require some licensees to develop and maintain a controlled badging and lock system to identify and limit access to the controlled access areas that store SNM of moderate and low strategic significance to authorized individuals.

Regulations in 10 CFR Part 73.55(e)(8)(C)(iii) require all emergency exits in the protected area to be alarmed and secured by locking devices that allow prompt egress during an emergency and satisfy the requirements of 10 CFR 73.55 for access control into the protected area.

Regulations in 10 CFR Part 73.55(e)(9)(ii) require licensees to protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements.

a. Unimpeded emergency egress should be ensured from all parts of the facility, and the security hardware and systems should be designed and installed so as to not degrade life safety. Security hardware and systems should conform to applicable (state and local) fire regulations and building codes. In recognition of the competing needs of safety and security, the 2012 edition of the National Fire Protection Association Life Safety Code (NFPA 101), (Ref. 27) suggests among other things, the use of "Key-Operated Locks" (Section 7.2.1.5) and "Special Locking Arrangements" (Section 7.2.1.6). The "Special Locking Arrangements" section includes provisions for delayed egress (Section 7.2.1.6.1) and access-controlled egress (Section 7.2.1.6.2). Each section has a number of specifications for the locking mechanism, its release, and identification. For example, under the Life Safety Code, a nuclear power plant would be classified as an "Industrial Occupancy" with a sub-classification of "Light",

"Ordinary" or "High Hazard." Light and ordinary industrial allow the use of special locking arrangements. Building codes often have similar requirements for egress while recognizing the need to provide security.

b. The following guidelines are acceptable for the selection and use of locks in the protection of facilities and SNM.

(1) Locks (locking systems) and all associated hardware should be properly installed, operable, and free of substantive indications of tampering. An explicit record should be maintained concerning such possible tampering marks and all service work rendered.

(2) The locks (locking systems) should be serviced and repaired by a regular employee competent in locksmithing or by a contractor locksmith whose assigned personnel have been processed or screened by the licensee for trustworthiness and reliability. Such processing or screening should be commensurate with that required for personnel granted unescorted access to vital areas or, as appropriate, the facility, SNM, matter, or information being protected.

(3) Combination locks installed in doors inside of, or leading to, areas containing classified matter should meet Federal Specification FF-L-2740 (if in vault doors) or should be pedestrian door deadbolts meeting Federal Specification FF-L-2890 (for doors to vault-type rooms). Combination locks on classified storage containers (GSA-approved security containers) should meet FF-L-2740.

(4) Locks on GSA-approved containers for arms and ammunition and armory vault doors should meet Federal Specification FF-L-2937 or UL 768, Group 1. The requirements of FF-L-2937 include the requirements of UL 768, Group 1. Locks that meet FF-L-2740 should not be used to protect weapons or ammunition in storage.

(5) Combination padlocks, rather than key padlocks, should be used when practical on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment. Combination padlocks should be used on closed vehicles or containers holding SNM that are required to be locked. These combination padlocks should be three-position, dial-type changeable-combination padlocks meeting Federal Specification FF-P-110.

(6) Key locks used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should provide a high degree of resistance to opening by force and tamper techniques and should meet the requirements of UL 437. A lock that meets Military Specification MIL-P-43607 with respect to 15-minute surreptitious neutralization resistance also could be used. Section B.2 of this draft regulatory guide describes two such locking systems.

(7) Key padlocks used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should be of rugged and sturdy construction and designed for outdoor use, if necessary, and should meet Federal Specification FF-P-2827.

(8) Locks used in the protection of Categories I and II SNM (e.g., security containers, safes, vaults) should meet Federal Specification FF-L-2740, "Locks, Combination." This is applicable to locks purchased or installed after the date July, 14, 1994, and for replacement of damaged equipment (Locks meeting FF-L-2890 also meet FF-L-2740).

(9) Electric locks should be used inside the protected area as a means of access control only if a magnetic card key system is coupled with a pushbutton system and integrated into the alarm system. This lock combination should have features that resist tampering with the combination-changing mechanism and that alarm after a set number of errors in entering the combination is made. Specifications for electric locks include UL 1034 and ANSI/BHMA A156.25-2002.

(10) Mechanical locks used as panic locks on emergency exit doors within protected area perimeters should be operable only from the inside.

(11) Mechanical pushbutton locks should be used inside the protected area as a means of access control and should comply with ANSI/BHMA A156.5-2001.

(12) For general purposes (no special requirements such as SGI, NSI, RD or SNM), emergency egress locks should comply with ANSI/BHMA A156.2-2003, "American National Standard for Exit Devices," (Ref. 28).

Regulations in 10 CFR Parts 73.46, "Fixed Site Physical Protection Systems, Subsystems, Components, And Procedures," and 73.50(c)(7) require licensees to control all keys, locks, combinations and related equipment used to control access to protected, material access, vital, and controlled access areas to reduce the probability of compromise. Whenever there is evidence that a key, lock, combination, or related equipment may have been compromised, the item shall be changed. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access shall be changed.

Regulations in 10 CFR Part 73.55(g)(6)(i) require the licensee to establish a system to control and inventory locks, keys, and combinations, including combinations to mechanical and electronic locks, mechanical keys, key cards, key codes, and all devices used for locking purposes.

The physical security plan, per 10 CFR 73.55(a)(2), shall describe a licensee/applicant site specific lock and key control systems provisions.

Keys not returned, as required under site specific conditions, may warrant the generation of a "Reportable Safeguards Event" per 10 CFR 73 Appendix G. The 10 CFR 73 Appendix G, requirement (c) "any failure, degradation, or discovered vulnerability that could have allowed surreptitious entry into a protected area, material access area, controlled access area, vital area, or transport, for which compensatory measures have not been employed" may be applicable. Applicability depends upon the specific type of licensee/applicant and protection the lock was providing.

c. The lock and key control system should include the following elements, where appropriate:

(1) A specific individual (usually a lock and key custodian) should be designated as responsible for all keys and locks, combinations, key cards, key codes, and keying records. All keys permanently assigned and not retained by the security organization should be receipted, and the key custodian should retain the original receipt.

(2) A record of all locks, cores, keys, and cards should be maintained and kept in a location secured by a combination lock. These records should be protected to the same degree or greater than the protection provided to the information, SNM, matter, or facility records being protected by the locks. This lock and key control register should identify the number of keys for each lock and their location and should note when a lock was changed, rekeyed, or rotated.

(3) A log of keys and key cards should be maintained that includes key identification, user, times issued and returned, dates, and other pertinent information.

(4) Keys, combinations, and key cards not in use should be protected adequately from theft, alteration, and measuring or reading.

(5) Keys and combinations should be issued only to individuals who are authorized users and whose official duties require use of the security key.

(6) The licensee should maintain, supervise, and annually review an authorized access list (i.e., those who require access to security keys) for this purpose.

(7) A lock and key control system should include procedures for verifying the identity of the individual requesting the keys or combinations and determining the individual is authorized access to all areas unlocked by the keys or combinations provided.

(8) Keys, key codes, key cards, and written combinations should not be removed from the site, except when specifically approved by the security plan.

(9) Keys should be issued daily, as required, and should be returned immediately thereafter or at the end of the duty shift.

(10) Only the required keys should be issued.

(11) Keys should only be issued to those persons who have the responsibility for accessing specific locations for their assigned conduct of business.

Regulations in 10 CFR Part 50, Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," specifically the requirement III N, require that the fire brigade leader shall have ready access to keys for any locked fire doors.

d. The fire brigade leader should be properly authorized for unescorted access to information, SNM, matter, or facility before granting access to keys that would provide such access. If the fire brigade leader is not authorized for unescorted access, procedures for escorting the fire brigade leader should be developed and personnel trained on the correct responses.

e. Beyond site specific persons who require access to certain areas, offsite persons may have the responsibility to have the ability to access certain site areas.

Per 10 CFR 73.70(h), each licensee subject to the provisions of 10 CFR 73.20, 73.25, 73.26, 73.27, 73.45, 73.46, 73.55, or 73.60 shall keep records of procedures for controlling access to protected areas and for controlling access to keys for locks used to protect special nuclear material. The licensee shall retain a copy of the current procedures as a record until the Commission terminates each license for

which the procedures were developed and, if any portion of the procedure is superseded, shall retain the superseded material for 3 years after each change.

f. Only the required keys should be issued.

(1) Keys should be inventoried during change of custody (usually each shift change).

(2) Master keying should not be practiced, except when safety and security considerations are an overriding factor.

(3) Any lock hardware removed from service should go directly to the locksmith responsible for the system or be secured.

(4) Unused locks, cores, keys, and cards should be stored in a location secured by a combination lock.

(5) The licensee should conduct an annual physical inventory of those locks, cores, keys, and cards used for the protection of facilities and a bimonthly inventory of those locks used for the protection of SNM. The lock and key control register should confirm the results of the inventory.

(6) The licensee should establish, and document in the physical security plan, a system for changing locks, keys, key cards, combinations, and related equipment. This should include a documented procedure by which to train personnel on the correct processes related to the following:

i. Licensees should change locks, keys, key cards, combinations, and related equipment used to control access whenever there is evidence that they may have been compromised. Determination of what constitutes possible compromise is subject to judgment; however, the security plan should describe factors to be considered. Generally speaking, compromise has occurred when an unauthorized person has gained internal access to a lock and its cylinder, been informed of its combination or code, gained possession of its key, or when a lock, key, key card, or written combination or code has been removed from the site without authorization or has been lost.

ii. Keys, key cards, key codes, combinations, and related equipment to which an employee had access should be changed upon termination or suspension of an employee's access authorization for any reason, including transfer. However, a licensee need not replace the affected locks.

iii. Locks should be immediately changed—or cores replaced and an inventory conducted—whenever a core, key, or card is lost or missing; the lock, core, key, or card has been compromised; or unrecorded keys or cards are found. In a mastered system, a complete remastering of the system should be conducted whenever a core, card, master or control key, or a lock is lost or compromised.

iv. Combinations should be changed before putting combination lock devices into service.

v. The licensee should change key codes and combinations for locks or padlocks used on repositories containing SNM or used on gates or doors to material access areas, in protected and vital area perimeters, and for access to vital equipment at least once every 6 months. Keys and locks should be changed or rotated at least once every 12 months.

vi. Deadbolts securing doors should have either a 1-inch lateral throw or use multiple vertical engagements with its strike.

vii. Outswinging doors and inswinging double doors without mullions should be equipped with securely mounted astragals or guard plates.

viii. Exterior or exposed cylinders should be rim, bored auxiliary or mortise lock mounted and should be protected with (1) a cylinder guard or (2) a substantial collar which is tapered, extends beyond the face of the cylinder, and rotates independently when torque is applied.

ix. When electronic locks are used on safety-related areas, the licensee should ensure prompt emergency ingress into the areas by essential personnel during any postulated occurrence by (1) using a combination of reliable and uninterruptable auxiliary power to the entire electrical locking system, including its controls, (2) providing the electrical locking devices, which are required to fail in the secure mode for security purposes, with secure mechanical means and associated procedures to override the devices upon loss of both primary and auxiliary power (e.g., key locks with keys held by appropriate personnel who know when and how to use them), or (3) providing periodic tests of all locking systems and mechanical overrides to confirm their operability and their capability to switch to auxiliary power.

D. IMPLEMENTATION

The purpose of this section is to provide information regarding the NRC's plans for using this regulatory guide and information on how the following entities ("applicants and licensees") may use this guide:

- applicants for, and holders of: (1) licenses issued under 10 CFR Part 70 to possess or use, at any site or contiguous sites subject to licensee control, a formula quantity of strategic special nuclear material, as defined in 10 CFR 70.4; (2) operating licenses for nuclear power reactors under 10 CFR Part 50; and (3) approvals issued under subpart B, C, E, and F of Part 52 ("protected applicants and licensees");
- applicants for, and holders of, operating licenses for nuclear non-power reactors under 10 CFR Part 50;
- applicants for, and holders of, licenses for industrial radiography under Part 34;
- applicants for, and holders of, licenses for medical use of byproduct material under Part 35;
- applicants for, and holders of, licenses for irradiators under Part 36;
- applicants for, and holders of, licenses authorizing the possession of an aggregated category 1 or category 2 quantity of radioactive material listed in Appendix A to 10 CFR Part 37;
- applicants for, and holders of, licenses for well logging under Part 39; and
- applicants for, and holders of, licenses, certificates, and other NRC approvals, who may safeguard Secret and Confidential NSI, RD, and FRD received or developed in conjunction with activities licensed, certified, or regulated by the Commission under Part 95.

In addition, this section describes how the NRC staff complies with the Backfit Rule found in 10 CFR 50.109(a)(1) and 10 CFR 70.76(a)(1), or any applicable finality provisions in 10 CFR Part 52, in its use of this regulatory guide.

Use by Applicants and Licensees

Applicants and licensees may voluntarily[1] 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**.** The acceptable guidance may be a previous version of this regulatory guide.

Licensees may use the information in this regulatory guide for actions that do not require NRC review and approval. However, voluntarily using the subject matter in the guidance may change a licensee's security plan such that NRC review may be required under the provisions of 10 CFR Part 50.54, 10 CFR 37.43, or 10 CFR Part 70.32, and should be evaluated prior to incorporating the methods into the security plan. Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

[1] 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.

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 any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request 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. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration for protected licensees.

During regulatory discussions on licensee-specific operational issues, the staff may discuss with licensees various actions consistent with staff positions in this regulatory guide, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting for protected licensees even if prior versions of this regulatory guide are part of the licensing basis. However, unless this regulatory guide is part of the licensing basis, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation.

If an existing licensee 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 revised 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 10 CFR 70.76(a)(1), or any applicable finality provisions in 10 CFR Part 52.

If a protected licensee believes that the NRC is either using this regulatory guide or requesting or requiring the protected licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the protected licensee may file a backfit appeal with the NRC in accordance with the NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection" (Ref. 29) and the guidance in NUREG-1409, "Backfitting Guidelines" (Ref. 30).

The backfit provisions in 10 CFR 50.109 and 10 CFR 70.76 and the issue finality provision in 10 CFR Part 52 do not apply to holders of licenses under Part 34, 35, 36, 37, 39, or 95, or holders of licenses for nonpower reactors under 10 CFR Part 50, unless those licensees also have an NRC regulatory approval under 10 CFR Part 50 (for a nuclear power reactor), 70, or 52, respectively.

GLOSSARY

ANSI—American National Standards Institute, the coordinator of America's voluntary standards system. The system meets national standards needs by marshaling the competence and cooperation of commerce and industry, standards developing organizations, and public and consumer interests. ANSI specifications listed in this manual have been adopted by the U.S. Department of Defense (DoD).

astragal—A member fixed to, or a projection over, an edge of a door or window to cover the joint between the meeting of stiles; usually fixed to one of a pair of swinging doors to provide a seal against the passage of weather, light, noise, or smoke.

auxiliary lock—A lock installed on a door or window to supplement a previously installed primary lock. It is also called a secondary lock. It can be a mortised, bored, or rim lock.

bevel (of a door)—The angle of the lock edge of the door in relation to its face. Bevel (of a latch bolt) is a term used to indicate the direction in which a latch bolt is inclined: regular bevel for doors opening in, reverse bevel for doors opening out.

BHMA—Builders Hardware Manufacturers Association . The association manufactures builders' hardware and publishes BHMA standards.

bolt—The part of a lock which, when actuated, is projected (or thrown) from the lock into a retaining member, such as a strike plate, to prevent a door or window from moving or opening.

case—The housing in which a lock mechanism is mounted and enclosed.

CFR—*Code of Federal Regulations*

control key—A key whose only purpose is to remove or install an interchangeable or removable core.

core—The innermost part of a key lock where the key is accepted. The terms "lock core" and "lock cylinder" are sometimes used interchangeably, but the cylinder is actually the part that surrounds the core.

cylinder—The cylindrical subassembly of a lock, including the cylinder housing, cylinder plug, tumbler mechanism, and keyway.

cylinder lock—

1. A lock in which the locking mechanism is controlled by a cylinder. A double-cylinder lock has a cylinder on both the interior and the exterior of the door.

2. A lock cylinder that has a threaded housing that screws directly into the lock case with a cam or other mechanism to engage the locking mechanism (mortise cylinder).

dead bolt lock—Any lock designed in such a manner that when the bolt is extended, it cannot be pushed back or opened with pressure against the end of the bolt.

double door—A pair of doors mounted together in a single opening.

knob—An ornamental or functional round handle on a door, which may be designed to actuate, lock, or latch.

latch—Any spring or mechanical device used to secure doors and other openings. Latches can be key- or lever-operated; they provide a low level of security.

latch (or latch bolt)—A beveled, spring-actuated bolt that may or may not include a deadlocking feature.

lock manipulation—The opening of the combination lock without alteration of the physical structure or disarranging of parts. Ordinarily, manipulation would be done by moving the lock dial.

master key—A key that will operate two or more locks that can also be operated with their own change keys.

master key system—A method of keying locks that allows a single key to operate multiple locks, each of which will also operate with an individual change key. Several levels of master keying are possible:

- A single master key is one that will operate all locks of a group of locks with individual change keys.
- A grandmaster key will operate all locks of two or more master key systems.
- A great grandmaster key will operate all locks of two or more grandmaster key systems.

Master key systems are used primarily with pin tumbler locks.

mortise lock—A lock in which the case is recessed into the edge of a door in a recess specifically cut out to receive it.

mullion—

1. A movable or fixed center post used on double door openings, usually for locking purposes.
2. A vertical or horizontal bar or divider in a frame between windows, doors, or other openings.

padlock—A detachable and portable lock.

security system—The compilation of all elements that make up the physical protection program necessary to meet 10 CFR Part 73 requirements, such as, equipment, personnel, procedures, and personnel practices, to include the way in which each element interacts with and effects other elements. (RG 5.76, "Physical Protection Programs at Nuclear Power Reactors.")

shackle—The movable part of a padlock that does the fastening.

strike—A metal plate designed to be secured to the door frame and accept the lock, bolt, or latch when the door is closed.

surreptitious entry—Gaining entry through a locked device or security container in such a manner that evidence of the act will not be readily discernible during normal operation of the locking unit or during inspection by a qualified person.

UL—Underwriters Laboratories, Inc. This nonprofit national testing laboratory tests and lists or labels various categories of equipment for safety and reliability. It also publishes standards for a wide range of products, including security products.

REFERENCES[2]

1. *U.S. Code of Federal Regulations* (CFR), "Domestic Licensing of Production and Utilization Facilities," Part 50, Title 10, "Energy."

2. CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Title 10, "Energy."

3. CFR, "Physical Protection of Plants and Materials," Part 73, Title 10, "Energy."

4. CFR, "Licenses for Industrial Radiography and Radiation Safety Requirements for Industrial Radiographic Operations," Part 34, Title 10, "Energy."

5. CFR, "Medical Use of Byproduct Material," Part 35, Title 10, "Energy."

6. CFR, "Licenses and Radiation Safety Requirements for Irradiators," Part 36, Title 10, "Energy."

7. CFR, "Protection of Category 1 and Category 2 Quantities of Radioactive Material," Part 37, Title 10, "Energy."

8. CFR, "Licenses and Radiation Safety Requirements for Well Logging," Part 39, Title 10, "Energy."

9. CFR, "Facility Security Clearance and Safeguarding of National Security Information and Restricted Data," Part 95, Title 10, "Energy."

10. U.S. Nuclear Regulatory Commission, "Access Control Systems," NUREG–1964, Washington, DC, February 2007. (ADAMS No. ML ML11115A078)

11. Lock Industry Standards and Training Council, "The Professional Locksmith Dictionary," 2006.

12. General Services Administration (GSA) Federal Specification FF-L-2740A, "Locks, Combination," January 12, 1997, including FF-L-2740A, Amendment 1, "Locks, Combination," May 25, 2001.[3]

---

[2] 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/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

[3] All current releases of the physical security directives and federal specifications listed herein are available electronically through the Documents section of the DoD Lock Program public Web site at https://portal.navfac.navy.mil/go/locks. Copies are also available from the DoD Lock Program at 1100 23rd Avenue, Port Hueneme, CA 93043-4370; telephone 800-290-7607, 805-982-1212, DSN: 551-1212; fax 805-982-1253; and e-mail NFESCLock-TSS@navy.mil. The physical security directives and Federal specification numbers and titles are based on their current editions. These documents will typically be updated, as needed, and be assigned a different title or number that addresses the same subject. These documents also are available electronically from the Web sites listed below:

13. Underwriters Laboratories, Inc. (UL) Standard UL 768, "Standard for Combination Locks," January 6, 2006.[4]

14. GSA Federal Specification FF-L-2890A, "Lock Extension (Pedestrian Door, Deadbolt)," April 1, 2004.

15. GSA Federal Specification FF-L-2937, Amendment 1, "Combination Lock, Mechanical," May 22, 2006.

16. GSA Federal Specification FF-P-110, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)," February 11, 1997, including FF-P-110, Amendment 1, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)," January 20, 2004.

17. National Archives and Records Administration, Information Security Oversight Office, *32 CFR Parts 2001 and 2004, RIN 3095-AB18, Implementing Directive No. 1, Final Rule*, Washington, DC, September 22, 2003.[5]

18. American National Standards Institute (ANSI) / Builders Hardware Manufacturers Association (BHMA) A156.5-2001, "American National Standard for Auxiliary Locks and Associated Products," March 27, 2001.[6]

19. MIL-DTL-43607H, "Padlock, Key Operated, High Security, Shrouded Shackle," March 10, 1998, U.S. Department of Defense Military Specifications, including MIL-DTL-43607H, NOTICE 1, "Notice of Inactivation for New Design, Padlock, Key Operated, High Security, Shrouded Shackle," May 22, 2000.

20. Underwriters Laboratories, Inc. (UL) Standard UL 437, "Key Locks," March 16, 2004.

---

[3] All current releases of the physical security directives and federal specifications listed herein are available electronically through the Documents section of the DoD Lock Program public Web site at https://portal.navfac.navy.mil/go/locks. Copies are also available from the DoD Lock Program at 1100 23rd Avenue, Port Hueneme, CA 93043-4370; telephone 800-290-7607, 805-982-1212, DSN: 551-1212; fax 805-982-1253; and e-mail NFESCLock-TSS@navy.mil. The physical security directives and Federal specification numbers and titles are based on their current editions. These documents will typically be updated, as needed, and be assigned a different title or number that addresses the same subject. These documents also are available electronically from the Web sites listed below:

Department of Defense (DoD): http://www.dtic.mil/whs/directives/
Department of Navy: http://doni.daps.dla.mil/default.aspx
Air Force: http://www.e-publishing.af.mil/
Army - http://www.army.mil/usapa/epubs/index.html
Federal Specifications - http://www.gsa.gov/portal/content/100847

[4] Copies of UL standards may be purchased from UL, 151 Eastern Avenue, Bensenville, IL 60106; telephone: Toll-free: 1-888-UL33512 or 1-888-853-3512. Purchase information is available through the UL Web site at http://www.ul.com/global/eng/pages/solutions/standards/

[5] The Classified National Security Information Directive No. 1 can be located at the public Web site at http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html

[6] Copies of American National Standards Institute (ANSI) standards may be purchased from ANSI, 1819 L Street, NW., Washington, DC 20036, on their Web site at http://webstore.ansi.org/; telephone (202) 293-8020; fax (202) 293-9287; or e-mail storemanager@ansi.org.

21. American Society for Testing and Materials (ASTM) Standard B-117 -07a, "Standard Practice for Operating Salt Spray (Fog) Apparatus," December 12, 2007.[7]

22. American Society for Testing and Materials (ASTM) International F883, "Standard Performance Specification for Padlocks," May 1, 2004.

23. GSA Federal Specification FF-P-2827, "Padlock, Key Operated, General Field Service," November 27, 2002.

24. MIL-DTL-29181, "Hasp, High Security, Shrouded, for High and Medium Security Padlock," U.S. Department of Defense Military Specifications, March 10, 1998.

25. UL Standard UL 1034, "Burglary-Resistant Electric Locking Mechanisms," February 23, 2000.

26. ANSI/BHMA A156.25-2002, "American National Standard for Electrified Locking Devices," January 24, 2002.

27. 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."[8]

28. National Fire Protection Association (NFPA) Standard NFPA 101, "Life Safety Code," 2012.

29. ANSI/BHMA A156.2-2003, "American National Standard for Exit Devices," October 15, 2003.

30. U.S. Nuclear Regulatory Commission, "Backfitting Guidelines," NUREG–1409, Washington, DC, June 1990 (ADAMS No. ML 032230247).

31. NRC Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," U.S. Nuclear Regulatory Commission, Washington, DC.

---

[7] Copies of ASTM standards may be purchased from ASTM, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959; telephone 610-832-9585. Purchase information is available through the ASTM Web site at http://www.astm.org.

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

BIBLIOGRAPHY

U.S. Nuclear Regulatory Commission Documents

Management Directive 12.1, "NRC Facility Security Program, Handbook."[9][10]

Management Directive 12.6 "NRC Sensitive Unclassified Information Security Program."

Management Directive 12.7 "NRC Safeguards Information Security Program."

NUREG-2155, "Implementation Guidance for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material"."[15]

NUREG-2166, "Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material."[15]

NUREG/CR-5929, "Locking Systems for Physical Protection and Control," November 1992. [11][12]

Other Documents

Executive Order 12829, "National Industrial Security Program," January 6, 1993. [13]

---

9 Management directives listed herein were published by the U.S. Nuclear Regulatory Commission. Division 12 directives are available electronically through the Electronic Reading Room on the NRC's public Web site, at http://www.nrc.gov/reading-rm/pdr/ref-materials.html#1.

10 Management Directives contain the policies and procedures that govern the internal NRC functions necessary for the agency to accomplish its regulatory mission.

11 NUREG/CR-5929 may be purchased through the U.S. Department of Commerce National Technical Information Service (NTIS) website at http://www,btus,giv/search/product.aspx?ABBR=NUREGCR5929.

12 NUREG/CRs are documentation of technical, regulatory, or administrative information about NRC programs or activities prepared by a contractor.

13 The National Industrial Security Program (NISP) or NISP Operating Manual may be found at http://www.archives.gov/isoo/policy-documents/eo-12829.html.

15 NUREG available on US NRC Website http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/