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

October 2016
Revision 1

Technical Lead
A. Tardiff

REGULATORY GUIDE

REGULATORY GUIDE 5.12

(Draft was issued as DG-5027, dated January 2015)

GENERAL USE OF LOCKS IN THE PROTECTION AND CONTROL OF: FACILITIES, RADIOACTIVE MATERIALS, CLASSIFIED INFORMATION, CLASSIFIED MATTER, AND SAFEGUARDS INFORMATION

A. INTRODUCTION

Purpose

This regulatory guide (RG) 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. Locks can be used in the protection of: areas, facilities, certain radioactive materials, and specific types of information (e.g., classified matter, National Security Information (NSI), Restricted Data (RD), Formerly Restricted Data (FRD), Safeguards Information (SGI)).

Applicable Regulations

- *U.S. Code of Federal Regulations*, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy" (10 CFR Part 50), (Ref. 1). Specifically Section 10 CFR 50.34 "Contents of applications" requires under (c)(1) that "[e]ach applicant for an operating license for a production or utilization facility that will be subject to §§ 73.50 and 73.60 of this chapter must include a physical security plan" and under (c)(2) "[e]ach applicant for an operating license for a utilization facility that will be subject to the requirements of § 73.55 of this chapter must include a physical security plan…"

- 10 CFR Part 50, Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," requires under III.N.4, that the fire brigade leader shall have ready access to keys for any locked fire doors.

- 10 CFR Part 52, "Licenses, Certifications and Approvals for Nuclear Power Plants" (Ref. 2). Specifically Section 52.79, "Contents of applications; technical information in final safety analysis report," requires under (a)(35)(i) the applicant to submit to the NRC a physical security plan that describes how the requirements of 10 CFR Part 73 will be met.

Written suggestions regarding this guide or development of new guides may be submitted 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/contactus.html.

Electronic copies of this 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/. The 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 ADAMS Accession No. ML15357A411. The regulatory analysis may be found in ADAMS under Accession No. ML16099A029, and the staff responses to the public comments on DG-5027 may be found under ADAMS Accession No. ML15357A410.

- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material" (Ref. 3). Specifically Section 10 CFR 70.22 "Contents of applications," requires under (h)(1) that licensees controlling a formula quantity of Special Nuclear Material (SNM) (except those licensed to operate a nuclear power reactor under 10 CFR Part 50) submit a physical security plan for NRC approval.

- 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel Independent Storage of Spent Nuclear Fuel, High-Level Waste, and Reactor-Related Greater than Class C Waste" (Ref. 4). Specifically Subpart H "Physical Protection" describes physical protection requirements, under Section:

    - 72.180, "Physical protection plan," requires that "[t]he licensee shall establish, maintain, and follow a detailed plan for physical protection as described in §73.51 of this chapter."

- 10 CFR Part 73, "Physical Protection of Plants and Materials" (Ref. 5), prescribes requirements for the establishment and maintenance of a physical protection system for the protection of special nuclear material at fixed sites and in transit. Specifically Section(s):

    - 73.22 "Protection of Safeguards Information: Specific requirements," under (c)(2) requires that SGI be stored in a locked Security Storage Container when unattended.

    - 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.

    - 73.46, "Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures," under (d)(14) and 73.50, "Requirements for physical protection of licensed activities," under (c)(7) requires licensees to control all keys, locks, combinations and related equipment used to limit access to protected, material access, vital, and controlled access areas, to reduce the probability of compromise.

    - 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level waste," under (d)(7) requires that, "[a] personnel identification system and a controlled lock system must be established and maintained to limit access to authorized individuals. "

    - 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," requires in subsection "(e) *Physical barriers*, under (4)," that "…openings in any barrier…" shall be "…secured and monitored to prevent exploitation of the opening…" commensurate with the intended function of the barrier.

    - 73.55 under (e)(8)(i)(C)(iii) requires 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.

    - 73.55 under (e)(9)(ii) requires 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.

- 73.67, “Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance,” requires licensees to, under (d)(5) “develop and maintain a controlled badging and lock system which identifies and limits access only to authorized individuals for controlled access areas that store SNM of moderate strategic significance,” and under (f)(1) utilize a controlled access area for activities involving SNM of low strategic significance.

- 10 CFR Part 20, “Standards for Protection Against Radiation,” (Ref. 6), specifically within Subpart I "Storage and Control of Licensed Material…”. Specifically Section(s):

  - 1801, “Security of stored material,” requires that “[t[he licensee shall secure from unauthorized removal or access licensed materials that are stored in controlled or unrestricted areas,”

  - 1802, “Control of material not in storage,” requires that “[t]he licensee shall control and maintain constant surveillance of licensed material that is in a controlled or unrestricted area and that is not in storage.”

- 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.

- 10 CFR Part 95, “Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,” (Ref. 8) specifically Section 95.25 “Protection of National Security Information and Restricted Data in storage,” under (a),(j) and Section 95.29 “Establishment of Restricted or Closed areas,” under (c)(3), describes licensee requirements to provide locks for the protection of classified matter and information.

Related Guidance

- RG 5.79, “Protection of Safeguards Information,” (Ref. 9) in Section C.4. “Protection While in Use or Storage,” within subsection (d).(2), provides related information on a “security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked as ‘GSA-Approved Security Container.’”

Purpose of Regulatory Guides

The NRC issues RGs 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 events, 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 RGs will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG contains and references information collections covered by 10 CFR Parts 20, 37, 50, 52, 70, 72, 73, and 95 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget (OMB), control

numbers (listed in the numerical sequence of the applicable Parts) 3150-0014, 3150-0214, 3150-0011, 3150-0151, 3150-0009, 3150-0132, 3150-0002, and 3150-0047.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

B. DISCUSSION

Reason for Revision

This revision of the guide (Revision 1) incorporates new information, lessons learned, and insights from operating experience since the original guide was issued in 1973, particularly information on new locking technologies and standards for locks and keys. Some specific items addressed include the some basic characteristics of a lock that licensees should consider when selecting locks, and information on when licensees should change combinations or keys. In addition, the revised guide cites updated references and describes relevant regulations, where appropriate.

Background

Locks can be an essential component of a physical barrier and consequently assist in meeting specific protection requirements. Locks assist in controlling access to areas, facilities, materials and information through doors, gates, and containers. 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 (examples include doors, gates, drawers) in a secured position. Locks are important components of a physical barrier; however, 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. However, the effectiveness of locks depends upon 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 access control systems. Lock componentry can consist of: physical latching systems for securing a movable portion of the security barrier, keys, and combinations. Access control systems, as described in NUREG-1964, include: identity verification devices, search procedures, search equipment, and locks. The elements of an access control system can consist of: procedures, access granting/denial hardware, contraband detection activities, computers, electronic databases, and associated detection, alarm, and communication infrastructures.

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 (for example, 0 through 99) and a three-number sequence (an example being "0-10-30") offers 1 million (100 x 100 x 100) combinations. Some combination locks require a four-number sequence (an example being "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-mounted lock, and the second is a padlock. High-quality combination locks are tested for resistance to surreptitious entry (examples are: manipulation, radiological analysis, and emanations analysis) and forcible entry.

Protection against forcible entry 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 entry. 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 (for example, 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 out-swinging doors and in-swinging double doors without mullions (for example, 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. Therefore, 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 replacing internal partsto change the combination.

Combination locks may be susceptible to compromise if the back of the lock is readily available (examples are: 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 re-entered 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. If the combination of a lock is changed by an intruder, that person would have access, but an authorized user would not. 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.

Both mechanical pushbutton and electronic (keypad) locks offer varying degrees of possible combinations and unsuccessful attempts. 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 result in wear patterns appearing on the pushbuttons, which could further reduce the number of combinations an intruder would need to enter to gain unauthorized entry. For electronic locks (keypads), a limited set of possible combinations can be balanced by limiting the number of unsuccessful attempts to access the lock (an example of this is after three 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. 12) 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 information. 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 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 should use a lock meeting the standards in Underwriters Laboratories (UL) 768, "Standard for Combination Locks" (Ref. 13) or locks meeting Federal Specification FF-L-2937, "Combination Lock, Mechanical" (Ref. 14). Locks meeting FF-L-2740 should not be used on field safes.

Figure 1. Field safe

Locks meeting FF-L-2740 resist 20 hours of manipulation, 20 hours of radiological analysis, 20 hours of emanations analysis, and 30 minutes of covert opening. Six locks have been approved under FF-L-2740: Mas-Hamilton Group models X-07 and X-08; Kaba Mas models X-09 and X-10; and Sargent and Greenleaf models 2740 and 2740B. All six models are electromechanical locks; the X-07, X-08, X-09, and X-10 are generator-powered, and the 2740 and 2740B are battery-powered. While all six models are approved, only the X-10 and 2740B are currently being produced.

Figure 2. X-10 lock

Pedestrian door deadbolts covered by Federal Specification FF-L-2890, "Lock Extension (Pedestrian Door, Deadbolt)" (Ref. 15) 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 FF-L-2890 consists of a mounting plate, a combination lock that meets

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 FF-L-2890, that feature single-motion egress for life safety, are available and applicable for protection of facilities approved for open storage of classified information. These locks can be integrated with a variety of access control systems.

Locks on GSA-approved containers and vault doors for securing arms, ammunition, and explosives should meet additional federal specifications. According to the U.S. Department of Defense Lock Program, mechanical combination locks should meet the latest revisions to the federal specifications listed below:

- FF-L-2937, "Combination Locks, Mechanical" (see Ref. 14)
- UL 768, Group 1, "Standard for Combination Locks."

Locks on GSA-approved containers and vault doors securing classified information, and on doors of facilities approved for open storage of classified information, should meet FF-L-2740. Locks on GSA-approved field safes should meet FF-L-2937 or UL 768, Group 1. Locks meeting FF-L-2740 should not be used on field safes.

Locks that meet the requirements of FF-L-2937 are available from the Defense Logistics Agency Troop Support. See the Mechanical Combination Lock Ordering Information page on its website for information on how to procure mechanical combination locks.
http://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock/SecurityHardware/CombinationLocks/ProductInformation/FF-L-2937_Locks/FFL2937_Order.html

Federal Specification FF-P-110, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)" (Ref. 16) covers changeable combination padlocks designed to conform to the standards for security equipment set forth in the "Classified National Security Information; Final Rule" (Ref. 17). These padlocks are required to resist opening for not less than 30 minutes by manipulation and 10 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 semi-protected by a structural overhang similar to eaves or a lean-to).

The standards in American National Standards Institute/Builders Hardware Manufacturers Association (ANSI/BHMA) A156.5-2014, "Cylinders and Input Devices for Locks," (Ref. 18) 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). A six-pin cylinder with ten depths per pin theoretically provides 1 million different keys. Beyond basic pin-tumbler cylinders, several high-security lock cylinders are available. These can provide increased resistance to

covert and surreptitious attack, as well as increased key control. They also can offer greater key control capability because the lock systems themselves and their key blanks should not be readily available commercially.

Licensees choosing to use master keying and interchangeable core systems should be aware of the susceptibilities created by such systems. 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 locks are not routinely monitored (e.g., a padlock on a gate at a remote site), the lock should not be master keyed, and the control key should be unique to that padlock. Control keys should only be issued to individuals authorized by the person in charge of the lock program.

Master keying should be done correctly to minimize the loss of security associated with such a system. Master keying is undesirable from a security perspective because any cylinder may be reverse-engineered to reveal the top master key. In addition, any compromise of a master key (e.g., termination of an employee who had access to a master key) compromises that entire master key system. Rekeying all the effected locks is costly, but because of the convenience of master key systems, there is strong desire to use them. A graded approach to this conflict, between convenience and security, could be to: (1) utilize a set of locks that has not been master-keyed for protected areas, material access areas, vital areas, and areas containing NSI, RD, FRD or SGI; and (2) use master-keyed lock sets for other, less sensitive areas. Master keying is prohibited for the protection of classified information or matter per 10 CFR 95.25(j)(8).

It is essential that the bolt of a lock is retained in the locked position by positive means, so that end pressure on the bolt will not retract it. 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 rapping or shimming defeat techniques (rapping and shimming techniques are common lock defeat actions), 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), designed by the U.S. Army, has acceptable forced entry protection. The PDLS is in compliance with Military Specification MIL-DTL-43607, "Padlock, Key Operated, High Security, Shrouded Shackle" (Ref. 19). 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.

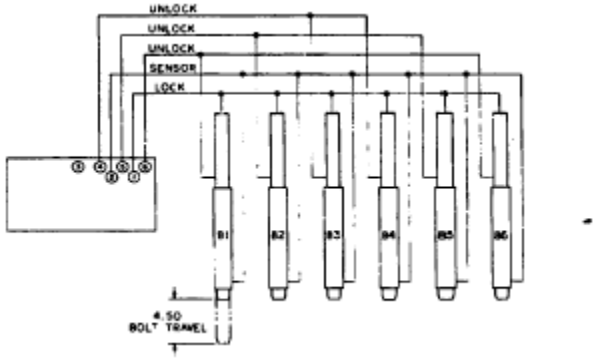

Figure 3. Pneumatic Deadbolt Locking System

UL 437, "Key Locks" (Ref. 20) covers door locks and locking cylinders, as well as other types of locks. It provides, for example, 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 the American Society for Testing and Materials (ASTM) International B-117-07a, "Standard Practice for Operating Salt Spray (Fog) Apparatus" (Ref. 21). For a complete description of all the tests a lock should pass in order to meet a certain lock specification, see the lock specification, for the lock of interest.

ASTM F883, "Standard Performance Specification for Padlocks," (Ref. 22) covers key-operated padlocks and has provisions for graded testing in terms of, for example, security, endurance (cycle test), and environmental attack.

Federal Specification FF-P-2827, "Padlock, Key Operated, General Field Service" (Ref. 23) covers key-operated padlocks intended for outdoor use. These padlocks are tested to the highest levels of environmental attack specified in ASTM F883 and provide moderate resistance to forced entry and picking.

MIL-DTL-43607 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. 24).

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 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 MIL-DTL-43607. The DoD has approved the 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 robust system will use two or more of these methods. A system using two technologies is

referred to as a two-factor authentication system. As an example of a two-factor authentication system, 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 facilitates protection against an observer perceiving the number sequence being applied. 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 (i.e., 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 is often accomplished by use of an electric strike. This is mounted in the frame, and the lock's bolt projects into it. The electric strike is released when electric current is sent to it, based on a valid opening signal (e.g., insertion of a valid credential). 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 lock system involves a person pressing buttons or switches to enter a code, a sight barrier should be installed to prevent observation of the code as it is entered. A system, in which each person presents a unique credential (e.g., an identification card with an electronic chip) and enters a unique personnel identification code, is more secure than a system that uses a single combination. In a unique credential only 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 a single combination system, if an employee were to retire or be debriefed from the program, all employees with access to the area would need to be given the new combination.

Pushbutton lock 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. 25) and ANSI/BHMA A156.25-2013, "Electrified Locking Devices" (Ref. 26).

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

Possession of locks, keys, key cards, combinations, and other related equipment by unauthorized individuals severely affects security and neutralizes the primary purpose of an access control program. In addition, information gained from spare locks and related equipment can allow unauthorized individuals to gain access. Licensees are required to control: (1) the distribution of keys, key cards, combinations, and locks; and (2) the storage of spare locks and related equipment (e.g., 10 CFR 73.22(a)(1)(6) locks combinations, mechanical key design, or passwords integral to the physical security system must be protected as SGI).

In order to implement such control measures, licensees should develop, implement, and maintain a formal process for distributing locks, keys, key cards, combinations, and related equipment to only authorized personnel. Furthermore, when an individual's authorization for access has been revoked or

suspended or has left employment duty, under less than favorable conditions, licensees should reduce security risk by: accounting for spare lock components, changing keys, denying function of specific access cards to key card processing systems, and changing combinations on certain lock systems.

Harmonization with International Standards

The International Atomic Energy Agency (IAEA) has established a compendium of publications which address 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 RG, IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/22/Revision 5)," (Ref. 27) addresses the recommended elements of a State's physical protection regime in the aspects of: use, storage, and transport of nuclear materials. This RG incorporates similar operational guidance and is consistent with the principles provided in the IAEA Nuclear Security Series No. 13.

Documents Discussed in Staff Regulatory Guidance

This RG 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 RG 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 RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a RG, 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

Locks may need to meet various federal specifications. In particular, 32 CFR 2001 (see Ref. 17), contains the most recent federal requirements to secure Secret and Confidential NSI, RD and FRD.

The regulation at 10 CFR 95.29(c)(3) requires that, during non-working hours, 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. When combination locks are used, the requirements of 10 CFR 95.25(c)-(f) apply. When key operated padlocks are used, the requirements of 10 CFR 95.25(j) apply.

In addition, licensees should consider complying with the National Industrial Security Program Operators Manual (NISPOM), DoD 52200.22-M, dated February 28, 2006, Incorporating Change 2, May 18, 2016, section 5-303 (Ref. 28), which states "SECRET material shall be stored in a GSA-approved security container, an approved vault, or closed area. Supplemental controls are required for storage in closed areas."

2. Selection and Use of Locks to Protect SGI

The regulation at 10 CFR 73.22(c)(2) requires SGI to be stored in a locked Security Storage Container when unattended.

Security Storage Containers, as defined in 10 CFR 73.2, "Definitions," "includes any of the following repositories: (1) for storage in a building located within a protected or controlled access area, a steel filing cabinet equipped with a steel locking bar and a three position, changeable combination, GSA-approved padlock; (2) a security filing cabinet 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; (3) a bank safe-deposit box; and (4) other repositories which, in the judgement of the NRC, would provide comparable physical protection." Therefore, besides utilizing a defined Security Storage Container for the storage of SGI, other proposed storage containers may be submitted to the NRC for approval.

Under 10 CFR 73.22(c)(2) 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 Safeguards Information in accordance with the provisions of this Section." Lock combinations to locks that protect SGI must be strictly controlled, per 10 CFR 73.22(a)(1)(vi), in order to prevent disclosure to an individual that is not authorized to access SGI.

Locks are required for the protection of SGI per 10 CFR 73.22(c)(2). Locks suitable for the protection of SGI include:

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

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

3. Selection and Use of Locks and/or a Lock and Key Control System to Protect Facilities/SNM under Part 73 (Radioactive Materials, Spent Nuclear Fuel, High Level Waste, SGI, NSI, FRD, and RD), and Administrative controls

For the protection of: (1) special nuclear material of a formula quantity, moderate strategic significance or low strategic significance, (2) a nuclear power plant, (3) classified matter/information or safeguards information, (4) spent fuel, (5) high level waste, or (6) quantities of radioactive material that fall under the jurisdiction of 10 CFR Part 37, a lock and key control system should be established. Key blanks and blank key cards can be of three types: (1) available to the public, (2) restricted access, and (3) unique to the site. A key blank or blank key card that is unique to the site may be numerically or alphanumerically stamped or otherwise configured in such manner that it is traceable by the licensee. Key blanks and blank key cards readily available to the public need not be recorded, controlled, and inventoried.

For licensees who are licensed to possess radioactive materials under 10 CFR Part 37 and/or 10 CFR Part 20, the guidance does not provide specific means to meet certain requirements, however the information within this RG as described in this section. may be useful in the development of a licensee's approach to meet security requirements.

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

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's standard termed the, "NFPA 101: Life Safety Code ®," (Ref. 29) suggests among other things, the use of "Key-Operated Locks" (Section 7.2.1.5.5), 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 occupancy 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 items as possible tampering marks and all service work rendered.

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

(3) Locks on GSA-approved containers and vault doors for arms, explosives and ammunition should meet 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 secure arms, explosives or ammunition in storage.

(4) 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 FF-P-110.

(5) 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. Locks should meet the requirements of UL 437, MIL-DTL-4360, or MIL-DTL-29181, with respect to 15-minute surreptitious neutralization resistance. Section B of this RG describes two such locking systems.

(6) 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 FF-P-2827.

(7) Locks used in the protection of Categories I (formula quantity) and II (moderate strategic significance) SNM (for example locks used on security containers, safes, vaults) should meet FF-L-2740 or FF-L-2890. This is applicable to locks purchased or installed after the date July 14, 1994, and for replacement of damaged equipment.

(8) 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 are made. When considering electric locks, the standards UL 1034 and ANSI/BHMA A156.25-2013 should be utilized.

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

(10) 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.

(11) For general purposes (no special requirements such as SGI, NSI, FRD, RD, radioactive material, spent fuel, high level waste or SNM), emergency egress locks should comply with ANSI/BHMA A156.2-2003, “American National Standard for Bored and Preassembled Locks & Latches” (Ref. 30).

Regulations at 10 CFR 73.46, 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.

Consistent with 10 CFR 73.46(d)(14), "… Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access, shall be changed."

Under 10 CFR 73.51(d)(7) licensees are required to " establish a "…controlled lock system…" in order "… to limit access to authorized individuals."

Furthermore, consistent with 10 CFR 73.55(g)(6)(i), "[t]he licensee shall control all keys, locks, combinations, passwords and related access control devices used to control access to protected areas, vital areas and security systems to reduce the probability of compromise."

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.

Keys not returned may warrant the generation of a "Reportable Safeguards Event" per 10 CFR 73.71, "Reporting of safeguards events." 10 CFR Part 73, Appendix G describes under I(c), a requirement that a reportable safeguard event is "[a]ny 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" and therefore may be applicable when keys are not returned. Applicability depends upon the specific type of licensee/applicant and protection the lock was providing.

c. Administrative controls for a 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, locks, combinations, key cards, key codes, and keying records. All keys permanently assigned and not retained by the security organization should be recorded and tracked by a receipt, and the key custodian should retain the original receipt.

(2) A record of all locks, cores, keys, key blanks, 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, matter, SNM, radioactive material, or facility records being protected by the locks. This lock and key control record 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: (1) key identification, (2) user, and (3) times/dates issued and returned.

(4) Keys, key blanks, combinations, and key cards not in use should be protected adequately from theft, alteration, and measuring or reading. For example keys, combinations and key cards not in actual use should remain in an individual's possession at all times and not left unattended.

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

keys should only be issued to those persons who have the responsibility for accessing specific locations for their assigned conduct of business. The licensee should maintain, supervise, and annually review an authorized access list (for example, those who require access to security keys) for this purpose.

(6) 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.

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

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

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

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

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

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

(13) The licensee should conduct an annual physical inventory of those locks, cores, keys, key blanks, 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 record should confirm the results of the inventory.

(14) In accordance with 10 CFR Part 50, Appendix R, Requirement III.N.4., the fire brigade leader shall have ready access to keys for any locked fire doors. The fire brigade leader should be properly authorized for unescorted access to information, SNM, classified matter, or a 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.

(15) Beyond site-specific persons who require access to certain areas, offsite persons may have the need to access certain site areas.

(16) 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 key blank, or when a lock, key, key blank, key card, or written combination or code has been removed from the site without authorization or has been lost.

ii. If an employee is transferred under less than favorable condition or has an access authorization terminated or suspended under less than favorable conditions, then the keys, key cards, key codes, control keys, combinations, and related equipment to which an employee had access should be changed. However, a licensee need not replace the affected locks.

iii. If 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, then locks should be changed or cores replaced and an inventory conducted as soon as possible. In a lock system that is master-keyed, a complete remastering of the system should be conducted whenever a core, card, master, control key, or a lock is lost or compromised. In addition, these change processes should be conducted after an employee who had access to these components of a lock/key system is terminated or loses access under less than favorable conditions.

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. Out-swinging doors and in-swinging 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.

For specific examples of how to secure radioactive material through the use of locks, in addition to the appropriate elements discussed in Section C.3. "Selection and Use of Locks and/or a Lock and Key Control System to Protect Facilities/SNM under Part 73, Radioactive Materials, Spent Nuclear Fuel, High Level Waste, SGI, NSI, FRD, and RD," there is information on how to secure radioactive material through the use of locks in NUREG-2155, Rev. 1, "Implementation Guidance for 10 CFR Part 37, Physical Protection of Category 1 and 2 Quantities of Radioactive Material," dated January 2015, (Ref. 31) and NUREG-2166, "Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material," dated May 2014 (Ref. 32).

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[1]") 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;
- applicants for, and holders of, licenses, certificates, and other NRC approvals, who protect safeguards information regulated by the Commission under 10 CFR 73.21-73.23; and
- applicants for, and holders of, licenses, certificates, and other NRC approvals, who may protect 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 backfitting provisions found in 10 CFR 50.109(a)(1) and 10 CFR 70.76(a)(1), or any applicable issue finality provisions in 10 CFR Part 52, in its use of this regulatory guide.

Use by Applicants and Licensees

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

---

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

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

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 50.54 or 10 CFR 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

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 without further backfit consideration for protected licensees. Examples of such unplanned NRC regulatory actions include issuance of an order requiring the use of the regulatory guide, issuance of generic communication, or promulgation of a rule requiring the use of this regulatory guide.

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 or applicant believes that the NRC is either using this regulatory guide or requesting or requiring the protected licensee or applicant 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 or applicant 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. 33) and the guidance in NUREG-1409, "Backfitting Guidelines" (Ref. 34).

GLOSSARY

access control— any barrier, device or administrative control, that limits or prohibits, free or unlimited access.

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. It is 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 and 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 storage container —Per 10 CFR 73.2 “Definitions,” a Security Storage Container is any of the following repositories:

- Within a building located in a protected or controlled assess area; a steel filing cabinet equipped with a steel locking bar and a three position changeable combination GSA-approved padlock;

- A security filing cabinet 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;

- A bank safe-deposit box; and

- Other repositories which in the judgment of the NRC would provide comparable physical protection.

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.

strikeplate—A metal plate designed to be secured to the door frame and accept the lock, bolt, or latchwhen 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 for-profit 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[3]

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

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

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

4. CFR, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel Independent Storage of Spent Nuclear Fuel, High-Level Waste, and Reactor-Related Greater than Class C Waste," Part 72, Title 10, "Energy."

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

6. CFR, "Standards for Protection Against Radiation," Part 20, Title 10, "Energy."

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

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

9. NRC, Regulatory Guide (RG) 5.79, "Protection of Safeguards Information," Washington, DC.

10. NRC, NUREG-1964, "Access Control Systems," Washington, DC, February 2007. (ADAMS No. ML11115A078)

11. Lock Industry Standards and Training Council, "The Professional Locksmith Dictionary," 2012.[4]

12. General Services Administration (GSA), Federal Specification FF-L-2740, "Locks, Combination Electromechanical," including Amendments.[5]

---

3 Publicly available NRC published documents are available online 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.

4 The lock dictionary may be found at http://www.locksmithingeducation.com/LIST_Dictionary.pdf

5 For all federal and military specifications, refer to the most current revision, which includes amendments (if applicable). Federal Specifications for locks could be found at: http://www.navfac.navy.mil/navfac_worldwide/lock program

Or Call the DoD Lock Program Technical Support Hotline:
(800) 290-7607, (805) 982-1212, DSN 551-1212
Other federal agency websites that may contain such information:
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/170591

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

14. GSA-approved, Federal Specification for FF-L-2937, Combination Locks, Mechanical, including Amendments.

15. GSA, Federal Specification FF-L-2890, "Lock Extension (Pedestrian Door, Deadbolt)," including Amendments.

16. GSA, Federal Specification FF-P-110, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)," including Amendments.

17. National Archives and Records Administration, Information Security Oversight Office, 32 CFR Parts 2001 and 2003, RIN 3095-AB63, Implementing Directive No. 1, Classified National Security Information, Final Rule, June 25, 2010.[7]

18. American National Standards Institute (ANSI) / Builders Hardware Manufacturers Association (BHMA) A156.5-2014 "Cylinders and Input Devices for Locks," January 24, 2014.[8]

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. UL, Standard UL 437, "Key Locks," March 16, 2004.

21. American Society for Testing and Materials International (ASTM), Standard B-117 -07a, "Standard Practice for Operating Salt Spray (Fog) Apparatus," December 12, 2007.[9]

22. ASTM 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.

---

6 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 Website at http://ulstandards.ul.com/access-standards/ Or http://www.comm-2000.com/Catalog.aspx

7 Copies of "*Classified National Security Information; Final Rule*" can be found at: http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.html

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

9 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.

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

26. ANSI/BHMA A156.25-2013, "Electrified Locking Devices," August 12, 2013.

27. International Atomic Energy Agency (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.[10]

28. National Industrial Security Program Operators Manual (NISPOM), "DoD 52200.22-M, dated February 28, 2006, Incorporating Change 2, May 18, 2016, section 5-303," May 2016.[11]

29. National Fire Protection Association (NFPA) Standard, "NFPA 101: Life Safety Code ®," 2012.[12]

30. ANSI/BHMA A156.2 -2003, "American National Standard for Bored and Preassembled Locks & Latches," July 2011.

31. NRC, NUREG-2155, Rev. 1, "Implementation Guidance for 10 CFR Part 37, 'Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material,'" January 2015.

32. NRC, NUREG-2166, "Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material," May 2014.

33. NRC, Management Directive 8.4, "Management of Facility-Specific Backfitting and Information Collection," October 2013. (ADAMS Accession No. ML12059A460)

34. NRC, NUREG-1409, "Backfitting Guidelines," Washington, DC.

10 Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its 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.

11 Copies of the National Industrial Security Program (NISP) Operating Manual, which incorporates change 2 from May 18, 2016, can be found at http://www.fas.org/sgp/library/nispom/nispom2006.pdf or by contacting the Federation of American Scientists, 1725 DeSales Street NW, Suite 600 Washington, DC 20036; e-mail fas@fas.org; phone: (202) 546-3300.

12 Copies of NFPA standards may be accessed through the NFPA website at http://www.nfpa.org/ or by writing National Fire Protection Association, 11 Tracy Drive, Avon, MA 02322, or Headquarters address: National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02269.

BIBLIOGRAPHY

U.S. Nuclear Regulatory Commission Documents

Management Directive 12.1, "NRC Facility Security Program, Handbook."

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

Management Directive 12.7, "NRC Safeguards Information Security Program."

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

Other Documents

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

13 The Executive Order 12829, January 6, 1993, "National Industrial Security Program" may be found at http://www.archives.gov/isoo/policy-documents/eo-12829.html.