Form 1221-002
(May 2022)

UNITED STATES
DEPARTMENT OF THE INTERIOR BUREAU OF LAND MANAGEMENT

HANDBOOK TRANSMITTAL SHEET

Release	9-436
Date	10/16/2023
Office Code	HQ-700

Subject: H-9173-2 – Minimum Security Requirements

FOIA Designation Letter: P

1. Updates, supersedes, or rescinds:

None. This handbook establishes minimum physical security requirements for the BLM's owned and leased facilities.

2. Explanation of Materials Transmitted:

The handbook is designed to provide minimum physical security requirements for planners, designers, engineers, and architects involved in new construction and major renovations to the BLM's owned and leased facilities. These minimum physical security requirements were derived from the Interagency Security Committee's Risk Managment Process.

3. Reports Required:

Include any internal or external reports required or state, “None.”

4. Delegations of Authority Updated:

Identify any changes to the delegation of authority made in the manual or handbook. Proposed changes to MS 1203, Appendices 1-20, must be provided to WO Directives, WO-830 and surnaming officials. Be specific on what appendix or appendices are affected by the change.

5. Filing Instructions: File as directed below.

REMOVE	INSERT
NONE	All of H-9173-2 (Rel. 9-436) (Total: 20 Pages)

Barbara Eggers
Assistant Director
Business Management and Administration

Table of Contents

Chapter 1 - OVERVIEW

A. Purpose

1. This handbook seeks to establish minimum physical security requirements for the Bureau of Land Management's (BLM) owned and leased facilities that have been designated as either Facility Security Level (FSL) I or FSL II facilities under the Interagency Security Committee's (ISC) criteria.

2. The information contained in this document can also be used as a general guide to secure facilities. It is not meant to be all-inclusive nor a replacement for the ISC Risk Management Process.

B. Background

1. Many facilities across the BLM will be designated either FSL I or FSL II facilities and are considered "occupied" as defined in 444 DM 1 *General Program and Physical Security Requirements*, which establishes the ISC's standards and guidelines as the basis for Department of Interior's (DOI) physical security program. Further insight into specific criteria for these designations is provided by the Department of Defense's Unified Facilities Criteria (UFC).

C. Applicability

1. This document should be used by the Physical Security POCs (Points of Contact) and others who are required or designated by State Offices and Centers to:

   a) Conduct Security Risk Assessments (SRAs); and

   b) Propose corrective actions to resolve deficiencies in a facility's current security posture and thereby reach the Achievable Level of Protection.

D. Authorities and References

1. 444 DM 1 *General Program and Physical Security Requirements*

2. MS-9173 rel. 9-435 Physical Security Program

3. H-9173-1 rel. 9-434 *Methodologies for Security Risk Assessment*

4. Permanent Instructional Memorandum 2022-043 The BLM's Physical Security Compliance Program

5. UFC-4-22 *Security Fences and Gates*

6. UFC-4-026-01 *Design to Resist Forced Entry*

7. UFC-3-530-01 *Interior and Exterior Lighting Systems and Controls*

8. UFC-4-021-02 *Electronic Security Systems*

9. Mary Lynn Garcia, *Design and Evaluation of Physical Security Systems*, 2nd edition

10. *Military Design Guidelines for Physical Security of Facilities,* MIL-HDSK-1013/1A (15 December 1993)

Chapter 2 – DEFINITIONS AND ACRONYMS

A. Definitions and Acronyms Associated with Physical Security Requirements

1. Access Control: One half of a system for allowing unescorted entry into Federal facilities, campuses, and sites. Access control consists of a favorable background check; a business need to access the facility, campus, or site; and issuance of a HSPD-12 credential.

2. CCTV System: Closed Circuit Television. Under the ISC criteria this kind of system is also known as a Video Surveillance System.

3. Clear Zone: Areas established interiorly and exteriorly to a perimeter fence line and designed to provide an unobstructed view to facilitate detection and assessment.

4. Common Access Door: A door that personnel commonly use for access into and out of a facility.

5. Compartment: A physically constrained area that can be configured to provide controlled access and prevent unauthorized entry.

6. The Five D's: Defend, detect, delay, deny, and deter.

7. Duress Alarm System: A duress alarm system is designed to protect individuals who may be subject to violence or other forms of attack or danger. The system typically consists of an SOS button or other device that can be used to send a duress signal to a monitoring center or security personnel.

8. Entry Control: The second half of a system for allowing unescorted entry into Federal facilities, campuses, and sites. Entry control encompasses the physical portion of the system and may consist of a hard key; electronic means or Physical Access Control System (PACS); or identification checks by unarmed or armed security officers. Included in this definition is the use of hard keys and locks. If the hard key and lock approach is adopted, there needs to be an accurate and up-to-date key roster, and periodic inventories should be performed.

9. Fail-Safe: Fail-safe doors become unlocked upon loss of electrical power. This means that if electrical power is lost, the door hardware is configured such that the door can be opened by anyone from the "public side." While affording great convenience, this configuration is vulnerable to intrusion during a power-loss event.

10. Fail-Secure: Fail-secure doors remain locked even with the loss of electrical power. This means that if electrical power is lost, the door hardware is configured such that the door cannot be opened/accessed from the public side. These doors need to be

keyed such that they can be manually unlocked by appropriate response personnel until the security panel and electrical power can be reset.

11. Glazing: Products constructed from laminated glass are referred to as having security glazing; they are designed to withstand the complex dynamic structural loads resulting from intentional impact or assault.

12. Hatch: An access point that is used for equipment or cable transfer into or out of a facility, including tunnels, basements, or channels. Hatches are commonly covered with a metal hinged plate. There may or may not be a ladder leading from the space or compartment to an access point.

13. Intrusion Detection System (IDS): An IDS is often referred to as a burglar alarm system. An IDS is designed to alert security personnel when unauthorized access is attempted. Alarm systems work in tandem with physical barriers and response elements (security officers/law enforcement), serving to initiate a response when these other forms of security have been breached. An IDS consists of types of sensors, such as motion sensors, contact sensors, and glass break detectors. In many cases, IDS and PACS are considered synonymous and are offered by vendors as an integrated unit or system.

14. Inoperable Windows (Fixed Window): A fixed window that cannot be unlocked, unlatched, or otherwise physically manipulated to create an "opening" as defined below. Such windows are not routinely considered physical access points to the interior of a facility. A solid pane or panes of glass associated with an inoperable window is considered a barrier to entry. Although it only minimally delays attempts to penetrate the interior of the facility, the window must be broken to create an "opening" that would allow physical access. The breaking of a window provides detection, upon discovery, that a potential malicious act or unauthorized physical access has occurred.

15. Occupied Facility: Facilities or structures occupied by DOI employees at least 50 percent of the time, where 50 percent occupancy is based on an average of 40-hour week (e.g., 20 hours per week per 12-month period or 40 hours per week for at least 24 weeks or 1,040 hours per 12-month period period). Appropriate security standards must be in place during that time of occupancy. All other facilities that have occupancy but do not fall under this "occupied" definition will comply with the requirements set forth for "unoccupied" facilities.

16. Opening: A hole or gap that can be physically breached. A maximum measurement of 96 square inches is the maximum allowable opening. Unprotected openings may be greater than 96 square inches if the narrowest part of the opening does not exceed 6 inches and the opening does not allow an intruder to pass through nor use a body part to gain unauthorized access. For example, a facility's window with the dimensions of 6' by 100" may not require protective measures. Securing openings that can be breached should include measures such as high-security locks, interior or welded

grates/coverings, interior or welded/pinned hinges, ladder guards, and so forth, so that all sides of the openings are tamper-resistant.

17. Operable Window: A window that can be unlocked, unlatched, or otherwise physically manipulated to create an "opening" as defined above.

18. Physical Access Control System (PACS): Electronic systems comprising card readers and other components that allow an individual unescorted authorized access to a facility or through a gate. In many cases, IDS and PACS are considered synonymous and are offered by vendors as an integrated unit.

19. Physical Security System (PSS): Consists of measures or sensors to *detect* an undesired event; *delay* or prevent an intruder from the commission of an undesired event; or determine how to *respond* to an undesired event. A response can consist of physical actions taken by employees, security personnel, or law enforcement before, during, or after an undesired event occurs. Alternatively, the response can be procedural in nature and involve notifying facility owners and/or property managers. A procedural response also includes policy guidance concerning how to recover from an incident and how to make assets resilient enough to withstand an incident.

20. Overhead Acting Door: Large roll-up or sectional doors that allow facility access by vehicles, or that create a facility opening to load/unload deliveries, equipment, or materials. These doors are not intended for routine ingress or egress.

21. Service Door: A door that is not commonly used for personnel access into a facility but is used periodically for servicing equipment; or a door that is required for emergency egress only.

Chapter 3 – ROLES AND RESPONSBILITIES

A. BLM Physical Security Specialist

1. Responsible for the formulation, review, and approval of minimum-security countermeasures to be employed at the BLM's owned and leased facilities, specifically for those facilities rated at a FSL I or II.

2. Reviews construction and major renovation projects to ensure that the minimum-security requirements contained in this handbook are included in the overall design of the facility.

B. State or Center Physical Security POC

1. Enacts the minimum-security requirements contained in this handbook.

2. Reviews construction and major renovation projects to ensure that the minimum-security requirements contained in this handbook are included in the overall design of the facility.

Chapter 4 – MINIMUM-SECURITY REQUIREMENTS

The following are the minimum-security requirements for all the BLM's occupied facilities. These requirements should be used as a template or checklist when conducting SRAs, and Deviation from the template should be coordinated with the BLM Physical Security Specialist.

A. The Five Ds for Planning, Designing, and/or Installing Factors for a PSS.

1. Defend: To defend a facility's perimeter against intruders requires the assistance of local law enforcement and on-site security personnel. To facilitate this cooperation, protocols should be established for the periods during and after a hostile act. Protocols should also be established for the period when a situation is being confronted by on-site security personnel prior to the arrival of local law enforcement.

2. Delay: Consists of interior and exterior locking doors and anti-personnel and anti-vehicle barriers. By having a delay system on-site, facilities give security personnel and local law enforcement additional time to respond to a criminal or hostile act.

3. Deny: To keep the perimeter secure while allowing authorized personnel to enter and exit, and to deny unauthorized personnel entry. A staffed security post at the physical access point can prevent those who do not possess a PIV card from entering the facility. Another way to deny entry to unauthorized personnel is to employ PACS. It is standard practice to utilize PACS to account for authorized personnel who are present in the facility.

5. Detect: Install on the facility's perimeter equipment that can detect trespassers. Surveillance cameras, motion sensors, and other security equipment that can sense movement are all essential to ensure that anything out of the ordinary is detected.

6. Deter: Generally, consists of signage that states "No Trespassing," "Property Under Surveillance," "Guard Dog on Premises," and "Security Personnel On-duty 24-7." While there may not be a guard dog, the suggestion of one could be enough to keep criminals at bay. Another line of deterrence is to have visible functional surveillance technology installed.

B. Physical Security Systems

1. Detection: Detection is enabled using security sensors such as door contacts, perimeter detection, motion sensors, and motion-activated CCTV, etc. For detection to occur, a means of determining if a hostile act is taking place is required. In most cases, this equates to the security sensor being under CCTV coverage along with proper lighting to aid in visual assessment. Additionally, the CCTV system should have playback capability enabling the operator to assess the activation of the security sensor and determine whether a hostile action has occurred. Continuous visual

observation by an employee or security officer is an acceptable alternative, but this method is inefficient and labor-intensive.

2. Delay: When properly installed, barriers such as fencing, security doors, cabling, large rocks, landscaping, and so forth can create a critically important delay. This delay can make assessment easier and provide time for a physical response by on-site personnel and/or local law enforcement.

3. Response: Responses to the activation of a security sensor after confirmation that a hostile act has occurred can be either physical or procedural. They can take the form of a security officer(s) physically responding to confront or intercept the bad actor; alternatively, responses can involve the use of a checklist or notifying a control center or local law enforcement via telephone.

4. Recovery: Recovery encompasses policies and plans that enable the return of an asset to operational (functional) capacity after an incident occurs; actions designed to regain command and control of an organizational response to an incident; and/or steps taken to regain control of an asset(s) that has been seized by bad actors.

5. Resilience: Resilience includes the construction or hardening of an asset to withstand the intended harmful effects of an incident; measures to promote the quick restoration of an asset to operational (functional) capacity; and/or procedures to shift resources from other locations to restore lost functional capabilities.

6. A properly designed and effective PSS must have the components of detection, delay, response, recovery, and resilience.

C. Access Control

To ensure effective access control, facilities should:

1. Create and maintain a comprehensive list of those requiring unescorted and routine escorted entry into the BLM's owned and leased facilities.

2. Establish a process to regularly update and validate the "Access List."

3. Create a process for the timely removal from the "Access List" of employees and persons who no longer eligible for unescorted and routine escorted entry to the BLM's owned and leased facilities.

4. Create a process to remove terminated and barred employees and contractors immediately from the "Access List."

5. Integrate the legitimate access list into the PACS database and authorized process.

D. Entry Control

1. A facility's minimum control method shall be the use of a physical key issued by the entity responsible for that facility.

2. The key control system shall implement controls, both physical and procedural, to reliably manage physical access to secure a facility or compartment.

3. The installation of PACS is required for FSL III and IV designated facilities and recommended for FSL I/II facilities.

4. PACS must meet the following specifications:

    a) FIPS 201-2.

    b) NIST Special Publication 800-116.

    c) Federal Identity, Credential, and Access Management Requirements.

    d) PACS components must be FIP 201-compliant and selected from the GSA's approved products list for PACS products.

    e) As an IT system, PACS must still be put through the Certification and Accreditation process, and an Authority to Operate must be obtained from the BLM before connecting PACS to the network.

E. Doors

1. General Requirements:

    a) Doors should be metal or solid wood. Additionally, locks, doors, doorframes, and accessory hardware are inseparable when the delay value of the door as a barrier is being evaluated.

    b) Exterior doors shall be commercial industry standard security rated doors constructed of metal, solid wood, or material sufficient to pass industry security standards.

    c) Exterior door frames shall be commercial industry security rated door frames and constructed out of metal and security mounted into the wall opening.

    d) Glass panels in doors:

        1. Shall be no larger than 96 square inches.

2. Glass panels in doors that are larger than 96 square inches shall have physical treatments to prevent unauthorized access or increase delay time for unauthorized access attempts. Physical treatments may include burglar-resistant film or glazing, security bars, and/or expanded metal mesh.

2. Exterior doors shall:

   a) Be capable of remaining locked when not in use.

   b) Have no window insert larger than 96 square inches, unless a specific architectural design is required for main facility entrances. In that case, the windows will require a security treatment such as ballistic glazing, anti-burglary glazing, metal mesh, or bars/grills. Such security treatments are applied to deter, and delay forced entry.

   c) Have latch protection (latch guards or astragals) installed at each door, or alternatively approved integrated latch protection.

   d) Have door hinges mounted on the inside of the door when possible. In cases where the hinges are on the outside, they will be peened, spot-welded, have screws installed, or be subject to other measures to prevent the removal of the door by removing the door hinge pins.

   e) When practical, be positioned in a manner that prevents direct observation of the interior of the facility. For example, an exterior door should not face or be directly adjacent to perimeter fencing or an installation’s defined boundary.

   f) Be designed to handle electrical power outages. In general, exterior doors should fail-secure for ingress and fail-safe for egress.

3. Common access doors must meet all life safety requirements. However, they shall control access by:

   a) Being equipped with a mechanical or electrical locking mechanism.

   b) Remaining locked when not in use.

   c) Ensuring that interior crash bars or panic hardware, door handles sets, or other devices cannot leave a door in a manually unlocked state.

   d) Having an automatic closing mechanism installed.

   e) Being equipped with door contacts (alarm points) for monitoring unauthorized access.

4. Service doors shall control physical access by:

a) Always remaining locked.

b) Being equipped with a mechanical locking mechanism.

c) Blocking physical access from the exterior of the facility. Physical treatments shall include installing door latch cover plates or astragals on the exterior side of the door and/or blocking physical access from outside the facility by removing or blanking all keyed access.

d) Ensuring interior crash bars, door handle sets, or other devices for egress cannot leave the door manually unlocked.

e) Having no external handles and being controlled by keyed, knob-less, deadbolt locks.

f) Having an automatic closing mechanism installed.

5. Overhead acting doors (roll-up and sectional garage doors) shall control physical access by:

a) Remaining locked at all times when in a closed state.

b) Not having unlockable levers or handles on the exterior side of the door.

c) Not allowing keyed access from the exterior of the facility.

d) Not enabling wireless remote opener devices (commercial or residential) to remotely open the roll-up doors.

e) Requiring authorized personnel to open the doors manually or electronically from inside the facility.

f) Ensuring that glass panels in roll-up doors meet the requirements found in paragraph 4.E.2. of this document.

6. A “Request to Exit” device will be installed in doors with an electronic lockset to disable the PACS forced door sensor when authorized personnel exit the door from the non-public side.

F. Inoperable Windows

1. Inoperable windows offer penetration resistance to or, in a worst-case scenario, evidence of unauthorized physical access. Physical treatments prevent unauthorized access or increase delay time for unauthorized access attempts. Physical treatments may include:

a) Forced-entry resistant laminated glazing. This treatment is recommended for all new facilities or facilities undergoing major renovations requiring new windows and window replacement.

b) Laminate that meets the standards outlined in ASTM-E-1886 and E-1996, Missile A Test Standards (flying debris).

c) Anti-intrusion/burglar resistant window film (for all existing windows that will not be replaced).

d) Film shall be integrated with the window frame.

e) Anti-intrusion film that meets the standards outlined in ATSM-F-1233, minimum protection level 1-1 shall be used.

2. Window frames should be securely anchored into the surrounding walls. Frames must not be removable from the outside in the areas under protection.

G. Operable windows

1. Operable windows shall be lockable from the inside when they do not need to be open for ventilation or other operational purposes.

2. Operable windows are physical access points into a facility unless these windows are rendered inoperable.

3. Operable windows create vulnerabilities which must be addressed, especially if the opening is greater than 96 square inches and the shortest dimension exceeds six inches.

4. Windows that can be routinely opened and are installed at a height less than 18 feet from any point adjacent to the window that permits unrestricted access shall be provided with protective measurements to deter or delay entry or to notify the response force of an attempted entry.

5. Windows that can be routinely opened and are installed at a height greater than 18 feet are not required to have security precautions installed.

6. If visual access is a security concern, the windows shall be rendered inoperable and treated with glazing that is translucent or opaque.

7. During non-working hours, the windows shall be closed and securely fastened to preclude clandestine entry.

H. Vents, Utility Openings, Hatches, and Other Points of Access

1. Potential entry points of access shall have a physical barrier installed that prevents access by blocking, barring, or screening off all openings to the facility greater than 96 square inches.

I. IT and Mechanical Rooms

1. Shall have solid floor-to-wall construction from the upper deck.

2. Shall have no unsecured openings of 96 square inches or greater.

3. Shall limit physical access to the minimum number of required personnel.

4. Shall have an electronic access card reader system installed (IT rooms only).

J. Key and Lock Standards

1. Key controls and inventory will follow the requirements outlined in *Military Design Guidelines for Physical Security of Facilities,* MIL-HDBK-1013/1A (15 December 1993) and UFC-4-026-01 *Design to Resist Forced Entry.*

2. The management of hard keys for a facility should be undertaken by a sole authority, such as a Physical Security Specialist, Facility Specialist, Administrative Officer, or the holder of some other authoritative position.

3. Key control programs will address processes for key issuance, annual accountability, and responding to the loss and destruction of keys.

4. Low-security padlocks (open shackle, key operable) must meet the classes and standards in Commercial Item Description A-A-59486B and A-A-59487B or another standard as approved by the BLM Physical Security Specialist.

5. Panic hardware or emergency exit mechanisms, if used on emergency doors located in secure areas, must be operable only from inside the perimeter and must meet all applicable Life Safety Codes.

6. Key locks for exterior doors and specific doors guarding access to sensitive areas should be six- or seven-pin (tumbler) locks and should have interchangeable cores.

K. Vehicle Gates

1. Vehicle gates shall be secured with an approved locking mechanism when not in use.

2. They will provide the same level of protection as the adjacent fence line.

3. When locked, they will not create a gap that would allow a person to slip through.

4. When locked, they will not create a ledge or step to assist a person in climbing over the gate.

5. They will not rely on hasps, hinges, or other hardware that, when closed, create a gap more than two inches wide.

6. Where possible, a shroud or hood will be installed to protect the gate lock from being cut.

7. Where chains are used to secure gates, ½-inch chains meeting or exceeding the requirements of Federal Specification RR-C-271 with approved padlocks will be used.

L. Pedestrian Gates

1. Pedestrian gates shall be secured with an approved locking mechanism when not in use.

2. They will provide the same level of protection as the adjacent fence line.

3. When locked, they will not create a gap that would allow a person to slip through,

4. When locked, they will not create a ledge or step to assist a person in climbing over the gate.

5. They will not rely on hasps, hinges, or other hardware that, when closed, create a gap more than two inches wide.

6. Where possible, a shroud or hood will be installed to protect the gate lock from being cut.

   Where chains are used to secure gates, ½-inch chains meeting or exceeding the requirements of Federal Specification RR-C-271 with approved padlocks will be used.

M. Perimeter Fence

1. Chain link fencing shall be designed and installed in accordance with UFC-4-22-03 *Security Fences and Gates.* The height of the chain link fence fabric should not be less than seven feet.

2. Based on regulatory requirements or based on the results of a SRA, medium security fencing may be installed for perimeter fence and gates. Refer to UFC-4-22-03 *Security Fences and Gates* for more details.

3. Facilities shall have a 20-foot minimum perimeter standoff distance between the facility and the physical security perimeter fence. Installing a new section of the perimeter fence or realigning the perimeter fence to include vehicle and/or pedestrian gate access shall be incorporated into the design/build activities, so that a 20-foot minimum standoff distance between the facility and the perimeter fence is maintained.

4. Depending on adjacent land uses, chain link or medium security fencing may not be appropriate. For portions of the BLM property directly affected by an incompatible land use, consider using other types of fencing. Decorative fencing shall meet site requirements. Refer to UFC-4-22-03 *Security Fences and Gates* for more details.

5. Clear zones, when required, will have varying dimensions depending on the asset being protected and the level of protection required. Where possible, outer clear zones should be 30 feet wide and inner clear zones should be 20 feet wide. These dimensions will be dependent on the availability of land. In all cases equipment should not be stored near perimeter fences to reduce the attractiveness of the site as a target for theft. Refer to UFC-4-022-03 *Security Gates and Gates.*

6. A top guard for a perimeter fence:

   a) Will be installed on the top of the perimeter fencing outward and upward at an angle of 45 degrees and will be 18 inches wide. The guard will add one foot to the height of the fence.

   b) For the guard, three or four strands of barbed wire spaced six inches apart are to be used.

   c) The length of the supporting arms and the number of strands used for the guard can be increased if an SRA reveals vulnerability.

N. Vehicle-Resistant Features

1. Perimeter fences and vehicle gates are not typically vehicle-resistant, making the asset vulnerable to a vehicle-borne improvised explosive attack.

2. To reduce the vulnerability while controlling the costs associated with vehicle-resistant fences and gates, installation of vehicle-resistant components may be deemed necessary based on an SRA recommendation, especially along likely avenues of approach. Such measures, which reduce the likelihood of fence and gate ramming, may include, but are not limited to, the use of:

   a) Aircraft cable.

   b) Bollards.

c) Jersey barriers.

d) Boulders.

e) Concrete planters.

f) Landscaping.

O. Signage

1. When required, facilities shall have signs announcing that the facility is Government property as well as Federal Property/No Trespassing signs. Refer to Title 41, Code of Federal Regulations (CFR), Part 102-74, for further information, and the BLM sign standard.

2. All facilities will have signage announcing what items are prohibited per Title 41, CFR Subpart 101-20.3.

3. When required, the "No Trespassing – Government Property" sign will be prominently displayed on all perimeter fences. One sign will be posted on each side at a maximum of 150-foot intervals and will be visible from outside the fenced area. Additional signs will be posted on all perimeter fences.

4. Federal Property/No Trespassing signs: Refer to 41 CFR 102-74 for further examples.

P. Lighting

1. When used for security purposes, lighting systems should provide a clear view of an area from a distance and enable anyone moving in or immediately around the facility to be easily seen, allowing for the identification of unauthorized persons. Lighting also serves as a deterrent to criminal activity, by creating the perception on the part of the unauthorized person that they can be seen.

2. Security lighting at most facilities will focus on three main areas: the facility's perimeter, especially entry and exits points; parking and roadway areas; and the facility's perimeter fence. Properly positioning the lighting ensures that it enhances the safety and security of personnel and property.

3. Security fence lighting design will should illuminate the external side of perimeter fencing, as well as the internal side.

4. Lighting should be selected and installed in a manner that does not degrade or inhibit CCTV effectiveness. For example, in most cases lighting should be as near as possible to "white light" in a natural light Color Rendition Index (CRI), and it should be installed above CCTV emplacements to prevent blooming or distortion.

5. An effort should be made to install the minimum amount of lighting needed to achieve the stated security goal. This will reduce light pollution and promote cost effectiveness.

6. Refer to UFC-3-530-01 *Interior and Exterior Lighting Systems and Controls* for more details.

Q. Duress Alarms/Systems

1. Duress alarms and systems are not required for most FSL I and II facilities but can enhance the security of personnel who interface with the public on a regular basis. Consider installing such systems when they are recommended by an SRA or use them as a mitigation when other countermeasures are not feasible.

2. Areas where a duress alarm or system should be considered include human resources sections, equal employment opportunity offices, managerial offices, and cash/public transaction areas.