Compassionate Certification Centers

PHYSICAL SECURITY HANDBOOK (PSH)

Cormier, Robert L

ERIGERE RAPIDUS SOLUTIONS, INC. 7 Donahue Avenue, Cherry Hill NJ 08002

Compassionate Certification Centers

Physical Security Program

Office of Security

Erigere Rapidus Solutions, Inc.

Chapter 1: Physical Security Program-Purpose

1.1 Purpose

1.1.1 Compassionate Certification Centers (CCC) has a duty to provide reasonable operating policies, procedures, and practices for the physical protection of personnel, infrastructures, and assets from deliberate and unforeseen threats at all their office locations.

1.1.2 These standards outlined in this policy shall be applied to all CCC facilities, owned, leased, or occupied space. Compliance shall be mandatory for all new construction, relocation, and renovation projects. Existing CCC facilities are not required to be upgraded unless a risk assessment determines otherwise.

1.1.3 These standards shall be used by CCC Management or their designated security contractor to serve as guide for: the development of threat assessments; evaluating security conditions during real estate market surveys and using the requirements guide for architectural and engineering (A&E) design efforts. Nothing in this policy handbook shall be construed as contrary to the provisions of any statute or other Federal, State or Local regulation. In the event of conflict, specific statutory provisions shall apply.

1.1.4 Physical Security Programs shall be administered based on the policy set forth in this handbook to ensure the protection of all CCC assets, patients and visitors. These programs shall be continually and effectively administered and monitored to ensure their integrity. At a minimum, a Physical Security Program shall include the items listed in **CHAPTER 2.1**

Chapter 2: Physical Security Program-CCC Policy

2.1 Policy

2.1.1 It is CCC's policy that personnel, facilities, property, information and other company assets shall be provided a consistent minimum level of protection. The minimum physical security standards provided in this CCC Physical Security Handbook (PSH) ensure a safe and secure work environment that contributes to the successful accomplishment of CCC's mission to raise the level of treatment patients receive while seeking their medical marijuana cards by providing trust, clarity, diagnostic help to find the right medicine. This policy includes but is not limited to:

- Development of minimum physical security standards for CCC Offices and regional facilities, by identifying requirements for all physical security systems, devices, and building features. These requirements shall be applied to new construction, renovation, and relocation projects, as well as projects involving security enhancements;
- Conduct of periodic surveys, inspections, and other formal on site threat and vulnerability assessments; and
- Participation in security projects managed by CCC's contract security firm. This includes the evaluating of CCC compliance with federal, state and local governments regulations and standards for physical security requirements.

2.1.2 All new construction, relocation and renovation projects must be coordinated through the CCC Security team to ensure compliance with applicable regulations and policies.

2.1.3 Proposed Changes or Revisions: It is intended that this handbook become a living document. As such, users of this policy handbook are encouraged to submit recommended changes and comments to CCC Management on the Appendix form marked: Policy and Procedures Handbook Comment. Comments shall reference the specific chapter and paragraph, and shall include a justification for the proposed change. Periodic revisions to this handbook will be published as necessary and to the extent practicable.

2.1.4 Protection Criteria: CCC Management and their designated contract security firm shall determine the level of normal protective service on a case by-case basis. The facility's location, size, number of occupants and configuration; history of criminal or disruptive incidents in the surrounding area-not primarily directed toward CCC's mission, the extent of exterior lighting, presence of physical barriers or other factors may be deemed pertinent and will be taken into consideration in the assessment.

2.1.5 Physical Protection: CCC shall provide normal and special protection through mobile patrol or fixed posts manned by contractually engaged uniformed personnel; security systems and devices; locking building entrances and gates during other than normal hours; cooperation of local law enforcement agencies; and a combination of these physical safeguards, depending upon the location and the degree of risk defined. The degree of normal and special protection is determined by completion of a ERS physical security assessment or crime prevention assessment and implementation of CCC's minimum standards contained in this policy handbook.

2.1.6 CCC shall delegate some of the protection responsibilities to the senior CCC manager having responsibility of the space. However, CCC Senior management shall be responsible for the procurement, installation, maintenance of physical security equipment and systems, and procurement and management of any guard contracts.

2.1.7 CCC Senior management is responsible for determining the degree of protection to be provided the space. The level of protection shall be based on a physical security survey of each facility conducted by ERS or other contract security service using the guidelines and requirements cited in this handbook to evaluate the security of that facility on a case-by-case basis considering the facility's location, size and configuration, number of occupants, and area's receptiveness of the mission.

2.1.8 Design Factors: It is imperative that security systems and procedures are considered from the start of the design phase so that conduit runs and alarm wiring, structural requirements, reinforcing devices and other necessary construction requirements are provided in the original plans.

2.2 Policy Exception Requirements

2.2.1 General: In rare situations where compelling operational requirements or conditions necessitate deviation from the specific minimum requirements in this handbook, CCC management shall:

- Document in writing any necessary exceptions from the requirements in this handbook prior to approval of the design concept;
- Complete, if possible, a mitigation plan that states what measures will be taken to minimize security vulnerabilities. Document how the proposed mitigation plan reduces risk to an acceptable level when compared to operational requirements; include persuasive evidence that the security of employees, assets and facilities will not be compromised by a less than standard facility;
- Include justification, risk analysis, cost comparisons, criteria applied, and other pertinent data. Lack of funds or cost savings do justify an exception, but all efforts shall be made to provide alternative security measures.

2.2.2 Exceptions that are approved will be for fixed term, unless specifically noted all exceptions will be granted for one fiscal year. At the close of a term of the exception CCC shall reexamine the security needs of the facility.

Chapter 3: Physical Security Program-Background

3.1 Background

3.1.1 Perimeter Security: Perimeter security standards pertain to the areas outside CCC control. Depending on the facility location, the perimeter may include sidewalks, parking lots, outside walls of the building, a hallway, or an office door. The elements of perimeter security are: parking, closed video surveillance system, lighting, and physical barriers.

3.1.2 Entry Security: Entry security standards refer to security issues related to the entry of persons and packages into a facility. The elements of entry security are: receiving/ shipping, access control, and entrances/exits.

3.1.3 Interior Security: Interior security standards refer to security issues associated with prevention of criminal or unwanted activity within the facility. This area concerns secondary levels of control after people or things have entered the facility. The long-term elements of interior security are employee/visitor identification, utilities, and occupant emergency plans.

3.1.4 Security Planning: Security planning is the development of long-term plans that incorporate requirements, standards, procedures, and processes to implement preventive and responsive countermeasures in the event of a breach of CCC security.

3.1.5 Security Planning: Sets security standards addressing broader issues with implications beyond security at a particular facility. The elements of security planning are: intelligence sharing, security awareness training, tenant assignment, administrative procedures, and construction/renovation.

3.1.6 Security Program: A comprehensive security system provides protection against a defined set of threats by informing the user of attempted intrusions and providing resistance to the would-be intruder's attack paths. This resistance must be consistent around the entire perimeter of the protected area.

3.1.7 Elements of Security Program: There are four main security elements that must be properly integrated to achieve a proper balance of physical security. These are:

- Detection: This is the process of detecting and locating intruders as far from the protected areas as feasible. Early detection gives the user more time for effective alarm assessment and execution of pre-planned response;
- Assessment: Assessment is determining the cause of the alarm or recognizing the activity. This must be done as soon as possible after detection to prevent the intruder's position from being lost;
- Delay: Intruders must be delayed long enough to prevent them from achieving their objectives before the response force can interdict them; and
- Response: A response force must be available, equipped, and trained to prevent the intruders from achieving their objective. The response time must be less than the delay time if the response force is to intercept the intruders before they achieve their objective.

Chapter 4: Physical Security Program-Supervision

4.1 Program Head-Chief Executive Officer

4.1.1 The Program Head: defined as the highest-ranking individual, is the Chief Executive Officer (CEO). The Program Head, in addition to other duties, is responsible for ensuring that security management duties, as defined in this CCC Physical Security Program manual, are carried out effectively and efficiently. The Program Head shall delegate duties as needed and detailed in the PSH.

4.2 Associate Program Head-Chief Operating Officer

4.2.1 The Associate Program Head: defined as the highest-ranking individual within the component of operations, is the Chief Operating Officer. The Associate Program Head is delegated the duties of the Program Head for operational purposes.

4.3 Office Management

4.3.1 Office Management: oversees a wide range of functions including day to day CCC operations and the direct supervision of the security program for CCC. Under the general supervision of the Associated Program Head, has been appointed to discharge these responsibilities.

4.4 Contract Security Personnel

4.4.1 Director of Security: Responsible for the design, implementation, testing and monitoring of the entire physical security program, internal investigations, background investigations and other duties as assigned;

4.4.2 Supervisory Security Officer: Responsible for overseeing the day to day operations of the Security Center (SC) which is responsible for life safety and emergency response in CCC offices and for Occupant Emergency Planning. Occupant Emergency Plans (OEPs) shall be required for all CCC facilities and include evacuation and Shelter-In-Place (SIP) protocols and procedures and encompass all hazards that may be encountered in the workplace (e.g., fire, severe weather, bomb threats, terrorism, and earthquakes). The Director of Security oversees the CCC emergency response plan, including emergency medical response, and delegates daily operations to the SSO.

Chapter 5: Physical Security Program-Facilities Protection

5.1 General

5.1.1 The degree of facility protection shall be determined by the Program Head, Associate Program Head and the Security Director based on the results of a comprehensive security assessment of the facility.

5.1.2 Perimeter protection is the first line of defense in providing physical security for personnel, property, and information at a facility.

5.1.3 The second line of defense, and perhaps the most important, is interior controls.

5.1.4 The cost of security controls above these minimum standards normally shall not exceed the monetary value of the item or areas to be protected, unless necessitated through an assessment

5.2 Planning Facility Protection

5.2.1 The objective of planning facility protection is to ensure the integrity of operations and the security of assets. Security planning must be an integral part of selecting, designing, constructing, reconfiguring, or moving into a CCC facility.

5.2.2 The modification of a facility or addition of security measures after occupying a facility can be costly and impractical. Therefore, the responsible Project Manager will coordinate from the outset, on any addition, alteration, or new construction with the Program Head. The coordination shall begin with the funding and concept phase, including the designers and architects and continue through the contracting process, actual construction, installation, and acceptance.

5.2.3 When CCC occupies leased facilities, it is imperative that the Program Head and Security Director establish a working relationship with the lessor and local law enforcement officials. If the leased property has a Building Association, both should be active at all meetings.

5.2.4 Facility Protection in CCC-owned or leased Facilities: The degree of protection to be provided for the space will be determined by the physical security assessment conducted by the Director of Security. The assessment will evaluate the security of that specific facility, taking into consideration the facility's location, size and configuration, history of criminal activity or disruptive incidents, extent of exterior lighting, presence of physical barriers, and other factors that may be deemed pertinent.

5.2.5 Protection Criteria: The Program Head and Security Director determine the level of normal protective service on a case by-case basis. The facility's location, size, number of occupants and configuration, history of criminal or disruptive incidents in the surrounding area, even those not primarily directed toward CCC's mission; the extent of exterior lighting, presence of physical barriers or other factors may be deemed pertinent and will be taken into consideration.

5.2.6 Physical Protection: Contract Security shall provide normal and special protection through mobile patrol or fixed posts manned by contractually engaged uniformed personnel; security systems and devices; locking building entrances and gates during other than normal hours; cooperation of local law enforcement agencies; or a combination of these, depending upon the facility and the degree of risk involved. The degree of normal and special protection is determined by completion of an ERS physical security assessment, crime prevention assessment, and the CCC minimum standards outlined in this handbook.

5.2.7 Crime Prevention: ERS collects and disseminates information about criminal activity in all areas CCC has established operations, and provides crime prevention awareness training to CCC upon request.

5.2.8 Facility Protection/Protected Property: In facilities that provide protection for their building, CCC shall delegate to the lessor as long as it is indicated in the lease agreement.

5.2.9 Design Factors: It is imperative that security systems and procedures are considered from the start of the design phase so that conduit runs and alarm wiring, structural requirements, reinforcing devices, and other necessary construction requirements are provided in the original plans.

5.3 Planning Facility Protection

5.3.1 The Program Head has determined that all CCC facilities shall meet a base line level of security. A higher level of security may be assigned to a facility based on the risk assessment conducted.

5.4 Facility Security Level Determination for CCC Facilities

5.4.1 New Leases in Existing Buildings: The appropriate security level for each lease requirement should be determined by the Program Head and Security Director.

- Where CCC anticipates making a new lease in an existing building (including succeeding lease actions), all of the Lease Security Standards (operating standards) listed for that security level must be met, with the exception of those requirments specifically prescribed under "New Construction-Standards";
- The standards shall be considered minimum requirements; and it is the intent that offerors unwilling or unable to meet the requirements should be considered non-responsive. A distinction should be drawn between operating standards and new contruction standards;
- Operating Standards : pertain to the operational and perhaps out sourceable nature of security, i.e. access control via guard service, VSS monitoring, magnotometers, x ray machines and HVAC security, to name a few. While the minimum operating standards must be met, existing buildings are not required to meet the standards required for new construction. CCC, at their own expense, may increase (but not decrease) the level of security in the Lease.
- Security Standards: As an example, a recommended security level for an office could be raised to a higher level, at CCC's request; or perhaps only a specific, isolated standard could be added to the office requirement.

5.5 Exterior Protection

5.5.1 Perimeter Security: Perimeter protection is the first line of defense in providing physical security for a facility. This can be accomplished by installing fences or other physical barriers, outside lighting, lockable gates, intrusion detectors, or a guard force. Perimeter protection also includes walls, lockable doors and windows, bars and grills, and fire escapes.

5.5.2 In addition to defining the physical limits of a facility and controlling access, a perimeter barrier also creates a physical and psychological deterrent to unauthorized entry. It delays intrustion into an area, making the possibility of detection and apprehension more likely. It aids security forces in controlling access and assists in directing the flow of persons and vehicles through designated entrances.

5.5.3 Every vulnerable point shall be protected to deter or prevent unauthorizede access to the facility. The roof, basement, and walls of a building may contain vulnerable points of potential entry. A security survey of the perimeter should address manholes and tunnels, gates leading to the basement, elevator shafts, ventilation openings, skylights, and any opening 96 square inches or larger that is within 18 feet of the ground.

5.5.4 The extent of the perimeter controls will be determined by the Program Head, based upon a comprehensive physical security survey conducted by the Director of Security. The survey report should recommend perimeter controls to the Program Head, if present. security control is required over public area and building entry points. This includes adjacent surface parking lots and structures under the building owner's control. Private tenancies shall be expected to comply. Security control means (generally) the right to inspect at point of entry and at any time present in the public space, the right to deny access and the right to remove vehicles from the premises;

5.5.5 Security control is obtainable by any of three (3) methods: Lessor furnished (turnkey), operating agreement (shared responsibility), or full leasehold control (ERS/Contractor furnished) depending on how the owners propose. CCC shall retain the right to provide security controls of their space at anytime during the lease term;

5.5.6 Garage control does not require CCC parkers, but may require some degree of garage management. Implementation of a vehicle pass/ID system for employee/contractor/patient parkers, acceptable to the CCC shall be required. Signage is required to alert parking patrons to inspection, surveillance and towing policies and removal of unauthorized vehicles;

5.5.7 Adequate Lighting: Protective Lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal or unapproved entry, and detecting intruders both outside and inside buildings and grounds. Locate protective lighting where it will illuminate shadowed areas and be directed at probable routes of intrusion. Also, overlap lighting to prevent dark areas. If justified, include emergency power for lighting. Where appropriate and determined by ERS/Contract Security, protective lighting with emergency power backup, for the exterior of the building shall be required. Parking areas shall be adequately lighted. 24-HR surveillance cameras (VSS) with time lapse video recording shall be required in lobbies and parking areas as deemed appropriate by the Security Director.

5.5.8 Windows: When appropriate, as deemed by the Program Head, applications of shatter resistant material, acceptable to CCC management, shall be applied on exterior windows in CCC occupied space. Windows are another vulnerable point for gaining illegal access to a building. Windows should be secured on the inside using a lock, locking bolt, slide bar, or crossbar with a padlock. The window frame must be securely fastened to the building so that it cannot be pried loose. As with glass panels in a door, window glass can be broken or cut so the intruder can reach inside and release the lock. Bars and steel grills can be used to protect a window. They should be at least one half inch diameter, round and spaced apart six inches to center. If a grill is used, the material shall be number nine

gauge two inch square mesh. Outside hinges on a window shall have non removable pins. The hinge pins shall be welded, flanged, or otherwise secured so they cannot be removed. Bars and grills must be securely fastened to the window frame so they cannot be pried loose.

5.5.9 Windows: When deemed appropriate by the Program Head, the Lessor shall provide and install wet glazed or mechanically attached, shatter resistant material not less than 0.18 millimeters (7-mil) thick on all exterior windows in CCC occupied space. The offeror shall provide a description of the shatter resistant window system in the attached Lessor Building Security Plan; and alternatively, when deemed appropriate by the Program Head the lessor shall provide certification from a licensed professional engineer that the window system conforms to a minimum glazing performance condition of 3B for a high protection level and a low hazard level. Window systems shall be certified by WINGUARD 4.1 or later or WINLAC 4.3 software to have satisfied the specified performance condition using the test methods in the ERS Security manual: ERS Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings.

5.5.10 Manholes, Grates, and Storm Drains: Many facilities have manholes and tunnels providing service entrance into buildings. Other manholes may provide entrance to tunnels containing pipes for heat, gas, water, and telephone. If a tunnel penetrates the interior of a building, the manhole cover shall be secured. A chain or padlock can be used to secure a manhole. Steel grates and doors flush with the ground level may provide convenient access. These openings may be designed into the facility as they may provide light and ventilation to the basement level. If the frame is properly secured, the grates or doors can be welded into pladce or they can be secured with a chain and padlock. Sewer or storm drains that might provide entrance shall be secured.

5.6 Exterior Protection

5.6.1 Physical Barriers may be of two general types: natural and man made. Natural barriers include: mountains, cliffs, canyons, rivers, or other terrain difficult to traverse. Man made barriers include items such as fences, walls, floors, roofs, grills, bars, or other structures which deter penetration. If a natural barrier forms one side or any part of the perimeter, it in itself shall not automatically be considered an adequate perimeter barrier, since it may be overcome by a determined intruder. Man made barriers shall be provided for CCC perimeters when deemed appropriate by the Director of Security.

5.6.2 Fencing: Fences are the most common perimeter barrier or control. Two types normally used are chain link and barbed wire. The choice is dependent primarily upon the degree of permanence of the facility and local ordinances. A perimeter fence should be continous, be kept free of plant growth, and be maintained in good condition. CCC shall determine if fencing is appropriate at a facility on a case by case basis.

- Chain Link: Chain Link fencing should be laid out in straight lines to permit unhampered observation. It should be constructed of number 9 gauge or heavier wire mesh material (Type I, II, or IV as defined in Appendix 6.7A, Fencing) with mesh openings (two inch square) and should be not less than seven feet high and have a top guard for a total of eight feet. Chain Link fencing shall extend to within two inches of firm ground. It shall be securely fastened to rigid metal posts set in concrete. Anti-erosion measures, such as surface priming, shall be applied when appropriate.
- Barbed Wire: Standard barbed wire is twisted, double strand, number 12 gauge wire, with four-point barbs spaced four inches apart. Barbed wire fencing, including gates intended to prevent trespassing, should be no less than seven feet in height plus a top guard, tightly stretched, and should be firmly affixed to posts not more than six feet apart. Distances between strands should not exceed six inches.

5.6.3 Gates: The purpose of a gate is to provide a break in a perimeter fence or wall to allow entry. Gates are protected by locks, intermittent guard patrols, fixed guard posts, contact alarms (IDS), VSS, or a combination of these. The number of gates and perimeter entrances should be limited to those absolutely necessary, but should be sufficient to accommodate the peak flow of pedestrian and vehicular traffic.

Gates should be adequately lighted. They should be locked when not manned and periodically inspected by a roving guard force. Utility openings in a fence that do not serve as gates should be locked, guarded, or otherwise protected. Intrusion detection devices (IDS) may be desirable when the gate is used intermittently or when a higher level of protection is desired. Alternatives to detection devices include coded card keys, push button combination locks, and VSS. For more information, see the section on Gates in Appendix 6.7B, Gates

5.6.4 Protective Lighting: Protective lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal entry, and detecting intruders both outside and inside buildings and grounds. Locate protective lighting where it will illuminate shadowed areas and be directed at probable routes of intrusion. Also, overlap lighting to prevent dark areas. If justified, include emergency power for lighting. For more information, see Appendix 6.7C, Protective Lighting.

5.6.5 Doors: A door is a vulnerable point of the security of any building. A door should be installed so the hinges are on the inside to preclude removal of the screws or the use of chisels or cutting devices. Pins in exterior hinges should be welded, flanged, or otherwise secured, or hinge dowels should be used to preclude the door's removal. The door should be metal or solid wood. Remember that locks, doors, doorframes, and accessory builder's hardware are inseparable when evaluating barrier value. Do not put a sturdy lock on a weak door. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other weaknesses that would allow entry. Transoms should be sealed permanently or locked from the inside with a sturdy sliding bolt lock or other similar device or equipped with bars or grills.

Overhead roll doors not controlled or locked by electric power should be protected by slide bolts on the bottom bar. Chain link doors should be provided with an iron keeper and pin for securing the hand chain. The shaft on a crank operated door should be secured. A solid overhead, swinging, sliding, or accordion type garage door should be secured with a cylinder lock or padlock. Also, a metal slide bar, bolt, or crossbar should be provided on the inside. Metal accordion grate or grill-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock. For more detailed information, see Appendix 6.7D, Doors and Hardware

5.6.6 Openings: Openings in elevators, penthouses, hatchways, or doors to the roof are often overlooked because of infrequent use. Access to a building's roof can allow ingress to the building and access to air intakes and building Heating, Ventilating, and Air-Conditioning (HVAC) equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof. From a physical security perspective, roofs are like other entrances to the building and should be secured appropriately. Roofs with HVAC equipment should be treated like mechanical areas. Fencing or other barriers should restrict access from adjacent roofs. Access to roofs should be strictly controlled through keyed locks, keycards, or similar measures. Skylights are another source of entry from the roof. These openings can be protected like windows - with bars or mesh. Such protection should be installed inside the openings to make it more difficult to remove. For further information see Appendix 6.7E Openings

5.6.8 Public Access to Mechanical Areas: Mechanical areas may exist at one or more locations within a building. Some mechanical areas have access from the perimeter; other mechanical areas may only have access from the interior of a facility. These areas provide access to centralized mechanical systems (HVAC, elevator, water, etc.) including filters, air handling units, and exhaust systems. Such equipment is susceptible to tampering and may subsequently be used in a chemical, biological, or radiological attack. Keyed locks, keycards, or similar security measures should strictly control access to mechanical areas. Additional controls for access to keys, keycards, and key codes should be strictly maintained.

5.6.9 Restrict Access to Building Operation Systems by Outside Maintenance Personnel: To deter tampering by outside maintenance personnel, a building staff member/contract security should escort these individuals throughout their service visit and should visually inspect their work before final acceptance of the service. Alternatively, building owners and managers can ensure the reliability of pre-screened service personnel from a trusted contractor.

5.6.10 Building HVAC Systems: Ventilation shafts, vents, or ducts, and openings in the building to accommodate ventilating fans or the air conditioning system can be used to introduce chemical, biological, and radiological (CBR) agents into a facility. Decisions concerning protective measures should be implemented based on the perceived risk associated with the facility and its tenants, engineering and architectural feasibility, and cost. Specific physical security measures suggested by ERS to consider for the protection of the building HVAC system are cited below.

5.6.11 Prevent Access to Outdoor Air Intakes: One of the most important steps in protecting a building's indoor environment is the security of the outdoor air intakes. Outdoor air enters the building through these intakes and is distributed throughout the building by the HVAC system. Introducing CBR agents into the outdoor air intakes allows an intruder to use the HVAC system as a means of dispersing the agent throughout a building. Publicly accessible outdoor air intakes located at or below ground level are at most risk – due partly to their accessibility (which also makes visual or audible identification easier) and partly because most CBR agent releases near a building will be close to the ground and may remain there. Securing the outdoor air intakes is a critical line of defense in limiting an external CBR attack on a building. Placement of the VSS can greatly assist in securing the area.

- Relocate Outdoor Air Intake Vents: Relocating accessible air intakes to a publicly inaccessible location is preferable. Ideally, the intake should be located on a secure roof or high sidewall. The lowest edge of the outdoor air intakes should be placed at the highest feasible level above the ground or above any nearby accessible level (i.e., adjacent retaining walls, loading docks, and handrail). These measures are also beneficial in limiting the inadvertent introduction of other types of contaminants, such as landscaping chemicals, into the building.
- Extend Outdoor Air Intakes: If relocation of outdoor air intakes is not feasible, intake extensions can be constructed without creating adverse effects on HVAC performance. Depending upon budget, time, or the perceived threat, the intake extensions may be temporary or constructed in a permanent, architecturally compatible design. The goal is to minimize public accessibility. In general, this means the higher the extension, the better – as long as other design constraints (excessive pressure loss, dynamic and static loads on structure) are appropriately considered. An extension height of 12 feet (3.7 m) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45 degrees is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes.
- Establish A Security Zone Around Outdoor Air Intakes: Physically inaccessible outdoor air intakes are the preferred protection strategy. When outdoor air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective alternative. Iron fencing or similar see-through barriers that will not obscure visual detection of intruder activities or a deposited CBR source are preferred. The restricted area should also include an open buffer zone between the public areas and the intake louvers. Thus, individuals attempting to enter these protective areas will be more conspicuous to security personnel and the public. Monitoring the buffer zone by physical security, VSS, security lighting, or IDS sensors will enhance this protective approach.

- Secure Return Air Grilles: Similar to the outdoor-air intake, HVAC return-air grilles that are publicly accessible and not easily observed by security may be vulnerable to targeting for CBR contaminants. Public access facilities may be the most vulnerable to this type of CBR attack. A building-security assessment can help determine, which, if any, protective measures to employ to secure return-air grilles. Take caution that a selected measure does not adversely affect the performance of the building HVAC system. Some return-air grille protective measures include (1) relocating return-air grilles to inaccessible, yet observable locations, (2) increasing security presence (human or VSS) near vulnerable return-air grilles, (3) directing public access away from return-air grilles, and (4) removing furniture and visual obstructions from areas near return-air grilles.
- Implement Security Measures, Such As Guards, Alarms, and Cameras to Protect Air Intakes or Other Vulnerable Areas: Difficult-to-reach out-doors air intakes and mechanical rooms alone may not stop a sufficiently determined person. Security personnel, barriers that deter loitering, IDS sensors, and observation cameras can further increase protection by quickly alerting personnel to security breaches near the outdoor air intakes or other vulnerable locations.
- Restrict Access to Building Information: Information on building operations – including mechanical, electrical, vertical transport, fire and life safety, security system plans and schematics, and emergency operations procedures – should be strictly controlled.

5.6.12 Fire Escapes and Building Walls: Normally, outside fire escapes do not provide an entrance directly into the building. However, they can provide easy access to the roof or openings high above the ground level. Windows or other openings off the fire escape shall be capable of being opened only from the inside. The exterior fire escape shall not extend all the way to the ground.

5.6.13 Walls are not normally considered possible points of entry because of their usual solid construction. However, they cannot be disregarded because intruders may be able to break through them to gain entrance. Reinforcement at critical points may be necessary to deter forced entry.

5.6.14 Facilities in Remote Locations: CCC facilities located in sparsely inhabited areas have an inherent form of protection by virtue of their isolation. Constructing a fence around the perimeter usually will provide an adequate deterrent to entry. Occasional observation by a roving guard force may be necessary depending on the crime index of the area. If deemed appropriate by the Director of Security, warning signs or notices shall be posed to deter trespassing on CCC property. VSS systems also can be especially helpful if guard forces are available to monitor them.

5.6.15 Exterior Signage: When deemed appropriate by the Program Head, Warning signs or notices shall be posted to deter trespassing on CCC property. Signs shall be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of such signs, lettering, and interval of posting must be appropriate to each situation.

5.6.16 Control Signs: Signs shall be erected where necessary to assist in control of authorized entry, to deter unauthorized entry, and to preclude inadvertent entry. Persons in or on CCC property shall be expected to comply with signs of a prohibitory, regulatory, or directory nature and with the lawful direction of security guards or other authorized individuals. Removal from CCC property for not obeying signage is permitted by Pennsylvania law.

5.6.17 Condition of Security Signs: Signs setting forth security of a CCC facility or area shall be plainly posted at all principal entrances and shall be legible under normal conditions at a distance not less than 50 feet from the point of entry. The signs shall state that: packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from CCC property, are subject to inspection at the discretion of CCC Management. Any person and vehicle are subject to a search at any time at the discretion of CCC Management and, if found to be in violation of federal, state or local laws, is subject to removal. This policy is in accordance with Pennsylvania laws pertaining to private property.

5.6.18 Restricted Areas: Signs or notices legibly setting forth the designation of restricted areas and conditions of entry shall be plainly posted at all entrances to such areas and at other points along the perimeter as necessary.

5.6.19 Explosives: Circumstances may dictate that CCC Management restrict certain types of material from offices. If applicable, signs or notices shall clearly indicate that no person entering or on CCC property shall carry or possess explosives, or items intended to be used to fabricate explosives or incendiary devices, either openly or concealed, except for official purposes.

5.6.20 Weapons Prohibited: CCC locations are private property and CCC management has legal authority to restrict and prohibit possession of a firearm or other dangerous weapon in CCC facilities, unless authorized by law. “Dangerous Weapons” is a weapon, device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing serious bodily injury or death, except that such term does not include a pocket knife with a blade of less than 2-1/2 inches in length.

5.6.21 Loading Docks and Service Access: Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible. For this reason, special attention should be devoted to these service areas in order to avoid undesirable intruders. Information on Loading Docks and Service Access may be found in Appendix 6.7F, Loading Docks & Service Access

5.7 Interior Protection

5.7.1 After exterior perimeter controls, the second line of defense is interior controls. When an intruder is able to penetrate the perimeter controls and the building exterior, the effectiveness of interior controls is tested. There are few facilities where every employee has access to every area in the facility. Accordingly, access to some areas is necessarily controlled. For example, interior controls are necessary to protect certain information from unauthorized disclosure, to prevent damage to the area or equipment, to prevent interference with operations, for safety purposes, or for a combination of these and other reasons.

5.7.2 Usually, interior controls are applied to specific rooms or physical spaces within a building. The Director of Security is responsible for determining whether interior controls are necessary. Office area controls include key accountability systems, locking devices and access control systems such as sign-in registers and identifying credentials. The Program Head shall approve interior controls based on a risk assessment completed by the Director of Security.

5.7.3 Costs: Determine the extent of interior controls by considering the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and the cost of the controls. Normally, the cost of security controls should not exceed the value of the item or areas to be protected.

5.7.4 Area Designations: The decision to designate areas as either a "Controlled Area" or a "Restricted Area" should be made by the Program Head in consultation with the Director of Security.

5.7.5 Controlled Area: A controlled area is defined as a room, office, building or other form of facility to which access is monitored, limited, or controlled. Admittance to a controlled area is limited to persons who have official business within the area. Responsible managers are authorized to designate an area as a controlled area after adequate security measures are in place. The following areas should be designated as controlled areas:

1. An area where protected information or highly sensitive information is handled, processed, or stored. A patient file room is considered such an area.
2. An area that houses equipment that is significantly valuable or critical to the continued operations or provision of services.
3. An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their duties.
4. An area where equipment or operations constitute a potential safety hazard.
5. An area that is particularly sensitive as determined by the responsible manager.

5.7.6 Restricted Area: A restricted area is a room, office, building, or other form of facility to which access is strictly controlled. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Visitors to a restricted area and un-cleared personnel must be escorted by personnel assigned to the area and all sensitive information must be protected from observation, disclosure, or removal. The responsible manager is authorized to designate an area as a restricted area after adequate security measures are in place. The following areas should be designated as restricted areas:

- An area approved by the Program Head for the storage of CBD Products;
- An area approved by the Program Head for the storage of sensitive patient records;

- An area designated by the Director of Security for the storage of security infrastructure;
- An area designated by the Program Head for the storage of any Medical Marijuana product, Schedule I/II Controlled Substance, or other protected medicinal item as defined by the Commonwealth of Pennsylvania and the DEA.
- An area designated by the Program Head for the storage of currency and proceeds.
- An area that houses mainframe computers or is designated IT sensitive systems.
- Any area that is determined to be highly critical or sensitive by a member of the CCC Executive Management team.

5.7.7 Access Control**: Vehicles and Traffic Control:** In the event of CCC having a controlled parking area these policies shall be applied at the discretion of the Program Head. If public vehicle entrances have gates, these will be manually opened and closed. Vehicle entrances with restricted access at facilities associated with a high threat level will be equipped with electrical or hydraulic vehicle gates or movable barriers. Vehicle barriers may be controlled by:

● Card readers;
● Biometric devices;
● Proximity tags;
● Electronic keypads;
● Line-of-site or using VSS; and
● One-way entry and exit lanes, created for high-traffic areas

5.7.8 Vehicle: In CCC facilities requiring large deliveries or parking areas controlled Vehicle loop detectors or other sensor systems may be used as request-to-exit devices, but must be located to prevent unauthorized activation. Vehicle screening may need to be conducted at locations associated with a high threat level. Screening is most associated with delivery vehicles entering a loading zone or dock area. At the discretion of the Program Head the screening area shall:

- Be at least 100 feet from the building;
- Have a one-way restricted traffic lane;
- Have signs and barriers to control traffic; and
- Allow vehicles to exit the inspection area safely if denied access.

5.7.9 Pedestrians: ACS systems shall be provided at public waiting and information areas, visitor areas, sally ports, secure vestibules, loading docks and entrances to restricted areas.

5.7.10 The access control system (ACS) may be a personnel, hardware, or computer based system:

- A personnel-based access control system relies on a person to positively identify individuals requesting access, determine if access is authorized, and secure the access point, ensuring that only authorized individuals have gained access.
- A hardware-based access control system uses mechanical push button or turn locks to gain access. This type of system is most suitable for interior areas with fewer than 25 users. Characteristics of this type of system are:
    1. One combination or the same key is used for all authorized individuals;
    2. No audit trail is available;
    3. No power is required; and
    4. A mechanical spring latch shall not be used as a lock-and-leave security measure.
- Automated Access Control Systems: are appropriate for large applications and may be required for programs associated with a high threat level. Systems may be in the form of stand-alone, one- or two-door units, small networks for 8 - 16 doors, or larger multi-door, multi-tasking systems. These types of systems are ideal for areas with 25 or more users and large systems controlling interior and exterior access control readers. Characteristics of this type of system are:
    1. All authorized users are provided with unique pass cards, tags or personal identification numbers (pins);

2. Audit trails are available;
3. Electrical power is required at each control point; and
4. Individual users can be deleted from the system without the need to recover cards, tags, pins or keys.

- Egress Controls: The decision to provide for controlled or uncontrolled egress will be based on a risk assessment of the facility. If it is determined that positive accounting of personnel or assets is required, controlled egress will be part of the access control system;
    1. The means of egress control will be at least equal to the access control for that portal;
    2. Door control applications must meet local fire codes; and
    3. Uncontrolled egress will likely be adequate for most area control points at the majority of CCC locations.
- Screening: All persons who are not CCC direct hires or full-time contract employees, are presenting themselves for an appointment as a patient or do not possess a valid building pass (if applicable) will be considered as visitors;
    1. All visitors requesting access to locations where a threat assessment has identified the need to screen for weapons, explosives, and incendiary devices will be screened; and
    2. Threat assessment may indicate a need to screen packages for weapons, explosives, and incendiary devices. Such packages may be transported by:
        - A Visitor Requesting Access;
        - A Freight Carrier;
        - An Express Package Delivery Firm;
        - The U.S. Postal Service;
        - U.S. Government/State Government Courier.

5.7.11 Routine Conditions/Requirements: During business hours, CCC facilities are normally open to the public and restricted to authorized individuals after business hours.

5.7.11 During business hours, property or portions thereof can be closed to the public if situations require this action to ensure the orderly conduct of CCC business. The decision to close the property or portions thereof to the public shall be made by the Program Head or designee after consultation with the local manager, Director of Security and the responsible Security Officer. When property or a portion thereof is closed to the public, admission shall be restricted to authorized persons who will register upon entry to the property and, when requested, display CCC or other identifying credentials when entering, leaving, or while on the property. Property or portions thereof that are closed to the public shall be designated as a restricted or closed area.

5.7.12 Emergency Conditions: During declared building security alert conditions, the display of CCC identification and additional screening may be required to enter the facility during all hours.

5.8 Area Designations:

5.8.1 The decision to designate an area as either a "Controlled Area" or a "Restricted Area" shall be made by the Program Head or designee in conjunction with the Director of Security.

5.8.2 Controlled Area: A controlled area is defined as a room, office, building or other form of facility to which access is monitored, limited, or controlled. Admittance to a controlled area is limited to persons who have official business within the area. Responsible managers are authorized to designate an area as a controlled area after adequate security measures are in place. The following areas shall be designated as controlled areas:

- Any area where sensitive information or highly sensitive information is handled, processed, or stored;
- Any area that houses equipment that is significantly valuable or critical to the continued operations or provision of services;
- Any area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties;
- Any area where equipment or operations constitute a potential safety hazard;
- Any area that is particularly sensitive, as determined by the responsible manager;

5.8.3 Restricted Area: A restricted area is a room, office, building, or other form of facility to which access is strictly controlled. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Visitors to a restricted area and uncleared personnel must be escorted by personnel assigned to the area and all classified information must be protected from observation, disclosure, or removal. The responsible manager is authorized to designate an area as a restricted area after adequate security measures are in place. The following areas shall be designated as restricted areas:

- Any area approved by the Program Head for the storage of Sensitive Information;
- Any area approved by the Program Head for the open storage of CBD Products, Medical Marijuana products, Schedule I/II Controlled Substances, and other sensitive products as defined by the Commonwealth of Pennslyvania, and the DEA.
- Any area housing the components of the IDS, ACS, and VSS security systems, and secure back up communications networks.
- Any area where sensitive information is visually displayed on an approved standalone office information system;
- Any area that houses mainframe computers or designated Automated Information System (AIS) sensitive systems; and
- Any area that is highly critical or sensitive, as determined by the Program Head or other responsible manager.

Chapter 6: Physical Security Program-Security Elements

6.1 Security Vault

6.1.1 Purpose: A vault is a completely enclosed space with a high degree of protection against forced entry. Vaults are commonly used for storing sensitive information, medical marijuana products, CBD products and extremely valuable materials and in some cases large amounts of currency. This section has been added to the CCC handbook in the event a decision is made to expand services requiring the use of a Class 3 Modular Vault. These are simply guidelines as CCC will not use a vault, rather a U.L. rated biometric safe.

6.1.2 General Requirements for Vaults and Vault Construction: A vault is constructed to meet rigid specifications. The wall, floor, ceiling construction shall be in accordance with nationally recognized standards of construction practice. An approved vault door and frame unit shall be used. Miscellaneous openings, where ducts, pipes, registers, sewer, and tunnels are of a such size and shape as to permit unauthorized entry (normally in excess of 96 square inches in area and over six inches in its smallest dimension), shall be secured by 18-gauge expanded metal or wire mesh, or where more practical, by rigid metal bars at least 1/2-inch in diameter extending across their width, with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and shall have crossbars to prevent spreading.

- There are three classes of vaults for the storage of sensitive material and equipment A, B and C.
- Class A Vault: this type of vault offers the maximum protection against tool and torch attack and shall have the following characteristics:
    1. Reinforced Concrete: The wall, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of a least 3,000 psi. Reinforcement will be accomplished with steel reinforcing rods, a minimum of 5/8 inches in diameter, positioned centrally and spaced horizontally and vertically 6 inches on center; rods will be tied or welded at the intersections. The

reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member;

2. Modular: Modular panel wall, floor, and ceiling components, manufactured of intrusion-resistant material, intended for assembly at the place of use, and capable of being disassembled and relocated meeting Underwriters Laboratories, Inc. (UL) standards are approved for vault construction.
3. Steel Lined: Vaults may be constructed of steel alloy-type, such as U.S. Steel T-1, having characteristics of high-yield tensile strength or normal structural steel with a minimum thickness of 1/4 inch. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction are less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

- Class B Vault: these vaults offer less than the max protection. A lightweight, portable "modular vault" may also be used to store sensitive material and equipment. The modular vault is equivalent to a Class B vault.
    1. Monolithic Concrete: The wall, floor, and ceiling will be a minimum thickness of four inches of monolithic concrete.
    2. Masonry Units: The wall will be brick, concrete block, or other masonry units not less than eight inches thick. The wall will extend to the underside of the roof slab above (from the true floor to the true ceiling). Hollow masonry units shall be the vertical-cell type (load bearing) filled with concrete and metal reinforcement bars. The floor and ceiling must be of a thickness determined by structural requirements, but not less than four inches of monolithic concrete construction.

- Class C Vault: offer less than maximum protection and may be used where unique structural circumstances do not permit concrete vault construction. The floor and ceiling must be of a thickness determined by structural requirements, but not less than four inches of monolithic concrete construction. Walls must be not less than eight inches thick concrete block or hollow-clay tile or other masonry units. The wall will extend to the underside of the roof slab above (from the true floor to the true ceiling).
- Utilization of any vault class, or the modular vault, is dependent upon the physical location environment where the vault is to be erected. The minimum construction requirements for each class of vault are described in detail in Appendix 6.10, Security Vaults.

6.2 Security Vault Doors

6.2.1 Vault doors and frames shall be rated a Class 5 Vault Door. All Security Vault Doors must be approved by the Contract Director of Security (ERS). ERS shall perform function testing to ensure compliance with applicable laws.

6.2.2 U.L. Rated: Underwriting Laboratories established and published uniform standards, and specifications for vault doors and associated security devices and equipment suitable for the storage and protection of sensitive information and materials. Vault door manufacturers and prices of equipment approved by ERS are available upon request. A vault door approved by ERS for storing sensitive information and material will bear a black "ERS Tested & Approved" label affixed to the exterior of the door and a "Class" label affixed to the interior.

6.2.3 Class 5 Vault Door: The class 5 vault door is certified for: 30 man-minutes against surreptitious entry; 20 man-hours against lock manipulation; 20 man-hours against radiological attack; and 10 man-minutes against forced entry.

6.2.4 Class 6 Vault Door: The certified class 6 vault door affords the same protection as the Class 5 except there is no certified forced entry protection.

6.2.5 Combination Locks: The ERS specifications and UL ratings for combination locks for vaults are the same as those for safes and storage equipment described in Chapter 7, Subsection 1, Paragraph 3: Types of Locks. The procedures for changing combinations,

protecting combinations, recording combinations, and repairing combination locks established in this handbook shall also be followed for vault doors.

6.3 Strong Rooms

6.3.1 Purpose: A strong room is an enclosed space constructed of solid materials. Strong rooms are normally used for the storage of sensitive information or sensitive materials, such as firearms and controlled substances. Protection is normally supplemented by guards or alarm systems. Rooms that have false ceilings and walls constructed of fibrous materials, and other modular or lightweight materials, cannot qualify as strong rooms without additional safeguards. CCC shall use strong rooms to secure security infrastructure, safes, and CBD storage.

- Construction Standards: The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration. Heavy-duty builder's hardware shall be used in construction. All screws, nuts, bolts, hasps, clamps, bars hinges, and pins should be securely fastened to preclude surreptitious entry. Hardware accessible from outside the strong room must be peened, brazed, or spot-welded to preclude removal.
- Additional Construction Standards: Walls and ceiling should be made of plaster, gypsum board, metal, hardboard, wood, plywood, nine-gauge or heavier two-inch wire mesh, or other material of sufficient strength or thickness to deter entry and/or give evidence of unauthorized penetration. Insert-type panels should not be used. Floors should be solidly constructed using concrete, ceramic tile or wood.
- Strong Room Windows: Windows, which open and are less than 18 feet from an access point (such as the ground, another window outside the area, roof, ledge, or door) should be fitted with 1/2-inch horizontal bars and cross bars (See paragraph above). In place of bars, number 9-gauge wire mesh can be fastened by bolts extending through the wall and secured on the inside of the window board. All windows, which might reasonably afford visual observation of classified activities within the facility, shall be made opaque or equipped with blinds, drapes, or other coverings.

- Where vents, ducts, registers, sewers, tunnels and other miscellaneous openings are of such size and shape (in excess of 96 square inches and over six inches in its smallest dimension) and enter or pass through the area as to permit unauthorized entry, they should be protected with either steel bars, expanded-metal wire mesh or grills, commercial metal sound baffles, or an intrusion detection system.
- Doors shall be substantially constructed of wood, metal, or other solid material. When windows, panels, louvers, or similar openings are used, they should be secured with 18-gauge expanded metal or wire mesh securely fastened on the inside.
- Entrance doors shall be secured by an ERS approved built-in three-position combination lock. Other (non-entry) doors shall be secured from the inside with deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door.
- For more information, see Appendix 6.12, Strong Rooms

6.4 Intrusion Detection Systems (IDS)

6.4.1 Purpose: Alarm systems are designed to alert security personnel of an actual or attempted intrusion into an area while also providing deterrence to intrusion. These warning systems detect intrusion or attempts, not prevent them. Any alarm system requires an assessment and a response capability to provide real protection for an area. All systems have weak points by which their functioning can be minimized or even completely interrupted or circumvented. The advantage and limitations of a variety of detection systems are described below.

6.4.2 Planning Alarm Installations: Alarms are used to detect approach or intrusion. Some are intended for exterior protection, and some are suitable only for indoor installations. The following should be addressed in determining the need for an alarm system:

- Sensitivity or criticality of the operation;
- Facility vulnerability to damage, interruption, alteration or other harm;
- Sensitivity or value of the information or property stored at the facility;
- Location of facility and accessibility of intruders;

- Other forms of protection in place or available; and
- Guard or law enforcement response capability.

6.4.3 Components of the Alarm System: An alarm system is composed of three main parts: one or more sensors to detect the presence or actions of an intruder, a control unit that constantly monitors the sensors and transmits an alarm signal when a sensor detects an intruder, and the alarm annunciator.

- Perimeter protection alarm systems utilize point protection sensors almost exclusively, while area protection (volumetric) sensors are used primarily in interior alarm circuits to detect an individual within a building. Object protection provides direct security for individual items and is often the final stage of an in-depth protection system with perimeter and area-protection.
- Alarm systems can be designed so that various parts of a building have separate sensor circuits, or zones, and it is not uncommon to have a separate duress or holdup alarm circuit to enable employees to summon security personnel.
- The installation of alarm system components is very important. Individual sensors are designed to respond to specific stimuli that indicate the presence of an intruder or attempts to gain entry into a protected area. Similarly, switch sensors must be mounted so that they detect the actual opening of a door or window, but at the same time, the manner of installation should not make them so sensitive to movement that they actuate an alarm from vibrations caused by a truck passing on the street or the wind rattling doors and windows. Care must be exercised in adjusting the sensitivity of the more complex sensors in order to avoid false alarms. Some units can be actuated by a flickering fluorescent light or a telephone bell. Electromagnetic interference from a mobile radio or a thunderstorm can trigger some detectors.

6.4.4 Sensors: The three basic types of sensors are perimeter, volumetric, and proximity.

- Perimeter: Perimeter protection is the first line of defense. The most common points for sensing devices are doors, windows, vents, and skylights. These may be protected with detectors sensing their opening or breaking. The major advantage of perimeter-protection sensing devices is their simple design. The major disadvantage is that they protect only openings such as doors or windows. If intrusion occurs through a wall or ceiling, these devices are ineffective.
    1. Switches: These devices are usually magnetic operated switches affixed to a door or window in such a way that opening the door or window removes the magnetic field causing an alarm. High security switches are normally balanced or biased magnetic switches.
    2. Metallic Foil: Metallic-foil window tape is the traditional means for detecting glass breakage. Strips of thin foil are affixed to a glass surface. Breaking the glass also fractures the foil, which interrupts the circuit causing an alarm. Metallic foil deteriorates with time and may require frequent maintenance, especially on glass doors where it can be easily damaged.
    3. Screens: Openings such as vents, ducts, skylights, and similar openings can be alarmed by thin wire filaments that signal an alarm if the screen is cut or broken. Often the wire filaments are placed in a frame of wooden rods and require little maintenance.
    4. Glass Breakage (Tuned Frequency): Miniature electronic circuits are bonded to the glass surface. They detect a high-frequency sound pattern within the glass when it is broken.
    5. Glass Breakage (Inertia): A device attached to window or doorframes protects multiple-pane areas. This device detects the shock w*ave a substantial impact against the surface makes.*
    6. Lacing: Lacing can protect walls, doors, and safes against penetration. Lacing is a closely woven pattern of metallic foil or fine brittle wire on the surface of the protected area. An intruder can enter only by breaking the foil or wire. A panel over the lacing protects it from accidental damage.

- Volumetric: Volumetric-protection sensors are designed to detect the presence or actions of an intruder almost anywhere within an entire room, from floor to ceiling. A variety of volumetric devices are available. Each kind of detector has some advantages and limitations. Therefore, a device must be selected for a specific environment. A major advantage of volumetric devices is that they provide a highly sensitive and invisible means of detection in high-risk areas. The major disadvantage is that an improper application can result in frequent false alarms.
    1. Infrared: Passive infrared sensors are part of the motion-detection group. They sense the body heat of an intruder as he or she passes through the protected area. Infrared detectors are relatively free of false alarms and are highly recommended.
    2. Ultrasonic: Ultrasonic motion detectors generate a high frequency of sound that is out of the normal range of human hearing. An intruder disrupting the ultrasonic wave pattern initiates the alarm. Ultrasonic devices are prone to false alarms due to excessive air currents or ultrasonic noise from mechanical equipment.
    3. Microwave: This kind of motion detector uses high-frequency radio waves, or microwaves, to detect movement. Because microwave penetrates materials such as glass, and metal objects reflect them, they can detect motion outside the protection area causing false alarm problems if not properly installed.
    4. Photoelectric: Photoelectric devices transmit a beam across a protected area. When an intruder interrupts this beam, the circuit is disrupted causing an alarm. Today's photoelectric devices use diodes that emit an invisible infrared light and usually pulses rapidly to prevent compromise by substitution. A disadvantage is that they can be defeated relatively easily, the beams are narrow and may be discovered or avoided.

- Proximity: Object protection provides direct security for individual items.
    1. Capacitance: A capacitance device is used to protect specific objects such as security containers and safes. The capacitance alarm uses the metal construction of the container and causes it to act as a capacitor or condenser. When a change occurs in the electromagnetic field surrounding the metal object, the balance is disturbed and the alarm is activated. The system can only be applied to ungrounded equipment and accidental alarms can occur if the container is carelessly touched when the alarm is activated.
    2. Vibration: These seismic sensing devices use a piezoelectric crystal or microphone to detect the sound pattern that a hammer-like impact on a rigid surface would generate. These devices are attached directly to safes and filing cabinets, or to the walls, ceiling, and floor of vaults. False alarms may occur with these devices by passing vehicles or falling objects.

6.4.5 Control Unit: All alarm systems incorporate a control unit, which may or may not be a separate component. The control unit is able to regulate the entire system, turn an alarm system on and off, and transmit the alarm signal to an annunciator. The method for controlling the alarm system is usually a key or a digital keypad inside the premises to avoid tampering. The alarm system is delayed briefly to allow the user to gain access to the system without initiating an alarm. With local systems, the user is responsible for turning the alarm on and off. The central station and proprietary systems shift responsibility for verifying that the system is on or off from the user to the central station or proprietary personnel. Alarm supervision falls into three categories: local, central station, and proprietary.

- Local Alarm System: The local alarm system has circuits within the secured areas that are directly connected to audio or visual signal-producing devices such as electronic annunciators, bells, or sirens. The signaling devices are normally mounted on the exterior of the building, or in large buildings at an interior location, where they will be audible or visible at a reasonable distance. It should be protected against weather or tampering.

- Central Alarm System: The central-station alarm system is connected to an alarm panel in a centrally located station such as a local police station or guard service that provides monitoring services over telephone lines. When an alarm is activated, the monitoring station initiates a response by either calling personnel designated for the area or by dispatching guards and/or police to the location.
- Proprietary Alarm System: The proprietary alarm system is similar to the central station type, except that the alarm panel is located in a manned guardroom on the protected premises. The guard force monitors the system and responds to all alarms. The alarms can also be wired to a central station or nearby police station via telephone wires for backup response.

6.4.6 Annunciator: An annunciator sounds an alarm by visible or audible signals and usually indicates the location of the protected item or premises. The alarm signal is transmitted to an annunciator panel that is constantly monitored or to a local signaling device. Local annunciators usually employ an audible bell, siren, and/or bright beams of light to deter the intruder and to attract the attention of persons in the immediate area. Annunciators may be combined in a system that announces alarms both locally and remotely.

6.4.7 Line Supervision: The telephone or dedicated lines that transmit the alarm signals from the protected area to the monitoring station must be protected to prevent interruption of the alarm signal. To ensure such integrity, the transmission lines should be electronically supervised. Line supervision refers to the protection various signaling techniques incorporate, such as random tone patterns or data encryption. The CCC IDS operates on its own digital cellular wi-fi network with its own 8-hour battery back-up to ensure coverage during interruptions of power or phone networks.

6.5 Video Surveillance System (VSS)

6.5.1 The Video Surveillance System (VSS) is another core subsystem of an overall Electronic Security System (ESS). It is a collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. The VSS system is normally integrated into the overall ESS and centrally monitored from the Dispatch

Center. Uses of VSS systems for security services include several different functions as described below.

6.5.2 Surveillance: VSS cameras can be used to give a viewer the capability to be made aware of, or view, visual events at multiple locations from a centralized remote viewing area. VSS camera technology makes visual information available that would normally only be available through multiple (possibly roving) human resources.

6.5.3 Detection: VSS cameras when employed with video content analysis or motion-path analysis, software and equipment, can be used as a means for intrusion detection.

6.5.4 Assessment: When alerted by an alarm notification, VSS cameras allow Dispatch Center operators or other viewers to assess the situation and decide as to what type of response may or may not be required. An example is an intrusion alarm at a remote facility. Visual assessment and other confirmation may indicate an unannounced maintenance crew at work. If it is determined that intrusion has occurred appropriate response would follow.

- Advantages are that one individual can monitor several VSS camera locations simultaneously; the image is visual and conveys much more information than other types of alarms; authorized individuals can be distinguished from unauthorized persons; and the signal can be recorded by a digital video recorder for playback and analysis at any later time, including a time-lapse mode for quick playback of lengthy periods of tape coverage. This system is often used in conjunction with a date-time generator, which can project a continuous image of the date and time in the corner of the monitor screen.
- Disadvantages are that monitors do not normally provide an alarm to alert the observer, the attention span of persons monitoring TV images is traditionally short, and there are often distractions at monitoring stations.

6.5.5 Deterrence: While more effective against unsophisticated burglars as opposed to trained covert insurgents, VSS cameras may deter burglary, vandalism, or intrusion due to fear of discovery and prosecution.

6.5.6 Evidentiary Archives: Retrieval of archived images may be helpful in identification or prosecution of trespassers, vandals, or other intruders.

6.5.7 Facial Recognition: Cameras can be used for biometric facial recognition.

6.5.8 Intrusion Detection: VSS cameras, when employed with video content analysis or motion path analysis software and equipment, are increasingly being used as a means for intrusion detection as discussed in Appendix 6.14, Intrusion Detection System

6.5.9 A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected or alarmed, such as a safe or a doorknob. When the image of an intruder or moving object enters the window, the difference in contrast is detected and triggers an alarm.

6.5.10 Emergency Alert Alarms: The teller's hold-up alarm in a bank is the most common illustration of an emergency alert alarm. Based on a risk analysis, emergency alert alarms should be considered at medical treatment facilities, personnel counseling or interview offices, credit unions, cash handling activities, and other high risk areas. The type and location of the device should be selected carefully to ensure the device is readily available for surreptitious activation in an emergency. If there is a building security force, a silent alarm should enunciate at the dispatch point. If not, the alarms can be monitored by a central station or direct connected to local police.

- The planned response to an emergency alert alarm must be designated to prevent endangering the occupants or creating hostage situations.
- Hold-Up Switches: The actuating device should be designed to avoid accidental actuation. Double squeeze buttons, triggers in trigger guards, and a variety of other devices can be used.
- Manual Switches: A hold-up alarm system in which the signal transmission is manually initiated by the person attacked activating the device. These alarms can be wireless.

- Automatic Switches: A hold-up alarm system that is automatically activated by device such as a money clip in a cash drawer.
- Foot Rails: A foot rail is an emergency alert alarm securely mounted on the floor and designed to minimize nuisance alarms, yet permit unobtrusive operation.
- For more detailed information, see Appendix 6.14, CCTV

Chapter 7: Physical Security Program-Locks and Keys

7.1 Locks

7.1.1 General:

- All exterior doors must have a lock with dead bolt or approved equal locking capability. All locks with a latch bolt must be equipped with a deadlocking latch feature. When specifying locks, use American National Standards Institute (ANSI) series lock numbers to obtain the proper type of lock for the function desired. The locks must meet all Federal handicap accessibility standards. All mortise locksets, whether or not required for security, must be grade one, commercial standard locks per ANSI/BHMA (Builders Hardware Manufacturers Association) A156.13. Unless specified, all interior non-security locksets may be cylindrical locks (bore lockset) as specified in ANSI/BHMA A156.2. The criteria in ASM 273.44, Postal Service Locks, also apply. Appendix 6.7.5, Doors and Door Hardware contains an approved list of panic-style entry and exit devices and high security devices;
- Some locks have interchangeable cores, which allow the same key system to include a variety of locks. Padlocks, door locks, cabinet locks, and electrical key switches can all be operated by the same key system. Because these cores are removable by a special key, this system allows for rapid re-keying of locks in the event that the key is compromised; and
- Locks are keyed in several different ways. When several locks are keyed differently, each is operated by its own key. When they are keyed alike, one key will open them all. Locks that are master-keyed are keyed differently, yet have one key that will open them all. Master-keying is done for convenience and

represents the controlled loss of security. Master-keying is not used unless permitted by the Program Head.

7.1.2 Locking Hardware:

- Locks are the most acceptable and widely-used security devices for protecting facilities, sensitive materials, and property. All containers, rooms, and facilities must be locked when not in actual use. Locking devices vary greatly in appearance as well as function and application. Locks merely deter or delay entry and shall be supplemented with other protection devices when a proper balance of physical security is needed. Some locks require considerable time and expert manipulation to open, but all locks can be defeated by force and with the proper tools. Locks must never be considered as a stand-alone method of security.
- For further information on locks and locking hardware, see Appendix 6.7.5, Doors and Door Hardware.

7.1.3 Types of Locks: Locks can be divided into three very general classes: (1) those that operate on purely mechanical principles; (2) those that are electro-mechanical and combine electrical energy with mechanical operations; and (3) electronic locks, which add to electro-mechanical lock devices various logic operations associated with integrated circuits.

- Mechanical Locks:
    1. Key locks consist of but are not limited to the following:
        a. Dead Bolt Locks: sometimes called tubular dead bolts. These are mounted on the door in a manner similar to cylindrical locksets. The primary difference is in the bolt. When the bolt is extended (locked), the dead bolt projects into the door frame at least one inch, and it cannot be forced back (unlocked) by applying pressure to the end of the bolt. The dead-bolt lock has the potential for providing acceptable levels of protection for storerooms and other areas where more security is desired. In situations where there is a window in or adjacent

to the door, a double cylinder dead-bolt lock (one that requires a key to open from either side) shall be used;

b. Mortise Locks: so named because the lock case is mortised or recessed into the edge of the door. The most common variety of mortise locks has a doorknob on each side of the door. Entrance doors often have an exterior thumb latch rather than a doorknob. Mortise locks are desired due to flexibility and can incorporate dead bolt without compromising fire or life safety compliance. Mortise locks for security must adhere to ANSI/BHMA A156.13 standards and must have a dead bolt with a minimum throw of 1 inch;

c. Stand-Alone Access Control Electro-Mechanical Locksets: are primarily used to control entry into an area. Rather than using a key, these open by pushing a series of numbered buttons. The locks can be either electrically or mechanically activated. Some of the advantages of using these locks are low cost, easy installation, easy combination changing, and simple operation. These devices are used for access control and do not provide a high degree of security when used alone. Some models have "time penalty" and error alarm features and can be tied to an existing alarm system. The combination or code used to activate an electro-mechanical door lock shall be changed at least every two years and when any person having knowledge of the combination no longer requires access to the area;

d. Padlocks and Detachable Locks: typically used with a hasp. Low security padlocks, sometimes called secondary padlocks, are used to deter unauthorized access, and they provide only minimal resistance to force. Low-security locks are made with hardened steel shackles. Precautions must be taken to avoid confusing these locks with similar brass or bronze locks. The brass or bronze locks are commonly used but do not meet the security requirements of the hardened shackled locks. High-security padlocks that meet ERS approval provide the

maximum resistance to unauthorized entry when used with a high security hasp;

e. Cylindrical Locksets: often called key-in-knob or key-in-lever locks. These are normally used to secure offices and storerooms. The locking cylinder located in the center of the doorknob distinguishes these locks. Some cylindrical locksets have keyways in each of the opposing knobs that require a key on either side to lock and unlock them. Others unlock with a key, but may be locked by pushing or rotating a button on the inside knob. These locks are suitable only for very low-security applications.

2. Additional Key Lock Specifications: All CCC lock cylinders must be of a high security, pick resistant design with angled key cuts, rotating tumblers, keyway side biting, and a slider mechanism. The cylinders must be Underwriters Laboratories (UL) listed under UL437 and certified under American National Standards Institute (ANSI)/Builder's Hardware Manufacturer's Association (BHMA) certification A156.30, Levels MIAM and ANSI/BHMA A156.5, Grade 1.
    - All cylinders must incorporate three locking elements: a slider mechanism, a sidebar mechanism with tumbler rotation, and a pin tumbler elevation. All cylinders must be constructed of solid brass with hardened steel inserts. The lock tumblers must combine a dual-axis action with one axis utilized for pin tumbler rotation and the other axis utilized for positioning key cuts. Randomly selected tumbler pins must incorporate a hardened steel insert. The cylinders must be capable of being immediately re-keyed to a new combination or a new system.
    - Interchangeable cores should be used to facilitate this process. A suitable number of spare cores should be maintained to facilitate lock changes in the event of a lost or stolen master key.
    - The manufacturer must have the capability of establishing a key system with a minimum of six angle cuts in six possible pin

positions with the capability of two distinct positions of cut per pin chamber, if required by the parameters of the system. The manufacturer must have the capability of producing a keying system in either of two distinct and different keying specifications and pinning specifications. The system must be capable of incorporating a key, with each being capable of more than one biting per position to expand master keying and key changes. The key must also incorporate the capacity to include twelve possible side biting along the key blade located on two different planes or surfaces of the key. The system must also have the capability to provide a single master key with over 1 million (1,000,000) usable, non-interchangeable change keys in a single keyway. The key thickness must be no less than one hundred, twenty-five thousandths (.125″) and must be made from a nickel silver alloy. Each key must be custom coined for tracking and identification purposes.

- The locking system must be deemed proprietary information shared only among authorized CCC entities and the manufacturer. Security Officers assigned to CCC and employees serving as in collateral security related functions, will have the authority to request additional pinning materials and duplicate keys.

3. Combination Locks: A manipulation-resistant combination lock provides a high degree of protection. It is used primarily for safeguarding classified or sensitive material. Its technical design is to prevent the opening lever from meeting the tumblers until the combination has been dialed.
    a) Built-in Combination Locks: When a security container or vault door is used to safeguard sensitive information, it must be equipped with a changeable 3-position, dial-type combination lock that has been approved by ERS/Director of Security. These locks can be purchased from companies identified by ERS.

b) Combination locks are classified as Group 1, Group 1 R, or Group 2

- **GROUP 1** - Those locks that have a high degree of resistance to expert or professional manipulation. The protection against expert manipulation includes advanced design features not found in conventional designs;
- **GROUP 1 R** - Those locks that have a high degree of resistance to expert manipulation, including use of radiological means; and
- **GROUP 2** - Those locks that have a moderate degree of resistance to unauthorized opening.

a) CCC shall use mounted combination locks, one for the protection of sensitive material and one for the protection of CBD and/or medical marijuana products. Combination locks that protect sensitive material must meet the requirements of Underwriters Laboratories Inc. Standard for Combination Locks UL 768, Group 1;

b) Combination padlocks approved by the Director of Security are intended for use as determined for low level resistance to forced entry and high level tell-tale manipulation or surreptitious action.

c) Combination Padlocks: Combination padlocks are locks designed for attachment to a mounted hasp. They are not approved for the protection of Schedule I/II Controlled Substances or HIPAA Information and are not rated for resistance to physical attack. Combination padlocks can be used either as a removable padlock in conjunction with bar-lock cabinets and other conventional hasp-type locks, or by fastening the security cover of the padlock to the surface of a container. It can be used on desks, storage cabinets, filing cabinets, sliding door cabinets, and virtually any type of

container through the use of an eyelet or loop designed to fit the tolerances of the opening of the padlock.

d) Protecting and Recording Combinations: The procedures for changing combinations, protecting combinations, and recording combinations are established in this handbook.

e) Combination to locks shall not be the same throughout any CCC facility, e.g. doors, vaults, etc.

- Changing Combinations: Combinations to locks installed on security containers/safes, perimeter doors, windows and any other openings should be changed by the responsible individual, the Security Officer, or by a bonded contractor immediately when:
    a) The container is placed in use;
    b) An individual knowing the combination no longer requires access to the container, unless other means of preventing exist;
    c) The combination has been lost or is suspected to have been lost;
    d) At least 12 months has passed;
    e) As directed by the manufacturer; or
    f) The container is taken out of service. Combinations to containers taken out of service must be reset to the standard factory combination of 50-25-50 prior to removal from the office space.
- Methods: Combination locks have either hand-change or key-change capability. Many combination locks produced by a variety of manufacturers have been approved by ERS. These ERS-approved locks along with the non-approved locks use slightly different operating instructions and unique keys or a particular hand change technique for changing combinations. Often the experience necessary, as well as change keys, operating instructions, and changing procedures, are lost with the passing of time;
- For assistance on lock issues contact ERS at info@erigererapidus.com or (800) 501-1035.

7.1.4 Selecting Combinations: When selecting combination numbers avoid multiples of 5, ascending or descending numbers, simple arithmetical series, and personal data such as birth dates and Social Security Numbers. Use numbers that are widely separated. This can be achieved by dividing the dial into three parts and using a number from each third as one of the high-low-high or low-high-low sequences. Use a unique combination for each container. Do not re-use this combination anywhere else in the same office. Carefully follow any manufacturers' instructions in installing combination numbers.

7.1.5 Protecting Combinations: Combinations should be known only by those persons whose official duties require access. The written combination should be protected at the highest classification level of material in the container or be protected in a manner commensurate with the value of the protected material;

- Combinations should be memorized. They must not be carried in wallets or concealed on persons or written on calendars, desk pads, etc.; and
- When opening any kind of combination lock, be sure that no unauthorized person can learn the combination by observing the sequence of numbers being entered or dialed. It may be necessary to position your body to block the dial from the view of anyone standing nearby.

7.1.6 Recording Combinations: ERS provides guidance, CCC internal personnel should assure that a record of the combination to each vault, secure room, combination padlock, and security container is recorded showing the location of the container or room, the name, home address, and home telephone number of a person responsible for the container. ERS Form ERS-700, Security Combination Information, has been designed for this purpose;

7.1.7 A central repository, usually the most secure container, should be designated to hold the sealed ERS-700 for use during emergencies. Only appropriately authorized employees should be given access to a combination. Combinations shall be controlled in the same manner as keys.

7.1.8 Electronic Locks: An electronic lock system uses a card key programmed with a code, which is read by a card reader that communicates with an automated central or local processor for access control. An electronic lock is considered a high-security lock according to the ERS. The card reader obtains data from the card by reading punched holes, magnetic strips or spots, imbedded wires, or any of several other methods. To open a door or activate a turnstile or lock, the card is typically inserted into a slot or groove and the coded area is read by the reader. If the code is an authorized one, the processor will direct the lock to open. Key cards should be voided in the system when lost, stolen, or when access is no longer required, and the card recovered.

- Electronic Card Readers: two basic categories: on-line and intelligent.
    1. On-Line Readers must communicate with a central processor that makes the entry/exit decision.
    2. The intelligent card reader compares the data on the card with preprogrammed data, and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or off-line readers.
    3. Multiple card readers can be used to control access to numerous buildings and rooms from one central processor. Most processors are capable of discriminating between time zones and levels of status for multiple readers and recording the time, date, location, and frequency of transactions. Many have additional features and capabilities such as monitoring alarms, keeping time and attendance records, and communicating with emergency or security personnel.

7.1.9 Biometric Systems: Biometric locking systems are available that use neither keys nor combinations. These include locks which open by using one of eight primary categories of biometrics technology: fingerprints, hand geometry, retinal scan, signature dynamics, voice verification, heat detection, facial recognition, or key stroke dynamics. These biometrics systems are primarily designed to control access to extremely sensitive, special-use areas where positive personal identification is an operational necessity.

7.2 Keys

7.2.1 General: This establishes the CCC policy and procedures for a standardized approach to the key management program, including administrative oversight, accountability, issue, receipt, duplication, replacement and documentation. This policy applies to all keys, all spaces, office equipment, vehicles, padlocks, lockers or other assets owned and operated by CCC and sets forth minimum standards.

7.2.2 Keys to locks are often the first and only level of physical security control for many organizational assets. Consequently, key control or the lack of it can mean the difference between a relatively secure activity and extraordinary loss. Almost all organizations utilize some type of key access in everyday operations. Each day offers an opportunity of key mismanagement, which can lead to mild annoyances such as the replacement and cost for lost keys, or to more serious losses, such as theft or personal injury. A good key control system will maintain a strict accountability for keys and limit both key duplication and distribution.

7.2.3 Key management and oversight helps protect life, property and provides a level of security to facilities and all occupants. Keys are the property of CCC and a part of physical security, which require strict control, management and accountability through keying systems integrity. Locks are the most common mechanism for access control on doors and security containers and often provide the primary protection against intrusion and theft. When a key is affected and/or compromised, the system is affected and compromised. Lack of an operational key control program can result in the compromise of personnel, property, and information. A functional key control program will ensure accountability; provide administrative oversight, and continuity of security through key issuance, duplication and replacement. Although a determined individual can open most key locks in a few minutes, they are used primarily to delay, discourage, or deter theft or unauthorized access. Exterior door locks shall at a minimum meet UL 437 standard.

7.2.4 The integrity of a key system is important to safeguarding property and controlling access. The security officer shall ensure that responsible individuals maintain control of the facility's key system by storing, issuing, and accounting for all keys. Issuance of keys must be kept to a minimum and only issued to persons who have an official need. Master keys must be carefully controlled; successful compromise of a master keyed installation can be very difficult and costly to remedy (assuming it is even discovered). Master keying systems can also incorporate a lock with a removable interchangeable lock core. Accurate accountability records must be kept, and all key records and documentation will be maintained for no less than one year. When keys are no longer needed they will be destroyed and documentation verifying destruction will be maintained.

7.2.5 A facility master key inventory and log will be maintained for chain of accountability and access control and will include as a minimum:

- The number assigned to each key and lock;
- How many keys per lock;
- Location of each lock, to include but not limited to room, container, or cage number; and
- Access list of persons authorized to use master keys.

7.2.5 Computerized Systems may be used.

7.2.6 The responsible person as identified by the Program Head or designee will approve and monitor all requests for issuance of new, duplicate, or replacement keys and ensure appropriate documentation is completed.

7.2.7 Physical Protection of keys will include, but is not limited to:

- Keys can only be stamped with blind control codes.
- Blind codes must not be reflective of buildings, door numbers or offices.
- Duplicate keys must be kept to a minimum, and when made the Master Key Inventory will be updated with required information;

- Non-issued keys must be safeguarded and controlled within a locked cabinet or container accessed only by the Key Control Person; and
- The key storage cabinet or container will be locked when not in use.

7.2.8 Employee Protection of Keys:

- CCC employees issued keys are to protect and secure them at all times, ensuring keys are not left on desks, in unlocked drawers, or where they can be easily taken and copied.
- Employees shall only use their keys to access their assigned work areas and shall lock doors when leaving any secured area;
- CCC employees assigned keys are not authorized to lend keys to individuals not specifically authorized;
- No person shall knowingly alter duplicate, copy or make a facsimile of any key to a lock of any building or property;
- The unauthorized possession, use or reproduction of any CCC key is a security violation; and
- A penalty shall be incurred for multiple losses at the discretion of the Program Head of their designee.

7.2.9 Types of Keys:

- Operating: sometimes called "change" keys; they are keys that are used to open locks.
- Duplicate: copies of operating keys and are usually stored for use in an emergency or to replace a lost key. Duplicate keys must be kept to a minimum and be protected to avoid proliferation and loss of accountability.
- Master: designed to open all locks of a particular series. Key systems can have one grandmaster key for the overall system and several sub-master keys for each subsystem. Master keys can be used as a convenience, e.g., carrying one key instead of numerous keys, but must be carefully controlled.

- Construction: open removable lock cylinders installed on the doors during construction of a facility. These cylinders are replaced at the end of construction with cylinders using the facility's key system.
- Control: are used to remove the cylinder of locks for changing keys. These keys are used only in interchangeable cylinder systems.

7.2.10 Key Issuance: A key issue form will be used to document in every instance of a CCC key issue and contain the following minimum criteria:

- Building number, floor number, room number, container number, or cage number;
- Key serial number;
- Key identification code;
- Quantity of keys issued;
- Brief statement of key control responsibilities;
- Printed full name of persons issued key(s);
- Organizational identifier of persons issued key(s);
- Signature of person issued key(s) acknowledging their key control responsibilities;
- Printed name of person issuing key(s);
- Signature of person issuing key(s); and
- Date key(s) issued.

7.2.11 Additional Key Issuance Guidelines: No person shall be issued multiple keys for the same area and in no case, shall the issuance of keys be authorized by the same person to whom the key is to be issued.

- Requirement for access does not constitute being issued a key, if other means are available for access. I.e., intercoms, request for entry, guards etc.;
- Keys shall be issued only to those individuals who have a legitimate and official requirement for the key;
- Keys are only issued to the occupant of the area, space or office or to a person they designate in writing; and

- Only the authorized recipient of an issued key may sign for that key and no other person.
- When assuming key control duties and responsibilities, the following minimum actions will be taken:
    1. All keys will be jointly inventoried every time a new key control person is assigned by both in-coming and out-going key control person and documented ensuring accountability;
    2. Inventory will be documented and both persons will sign accountability document; and
    3. Inventory will include both individual's name and signature, date of inventory, any discrepancies found and actions taken.

7.2.12 Key Return: Keys will be returned to the Key Control Person upon the departure or reassignment of any person who was issued a key(s), and will not be given to any other individual for use or turn-in. Any person returning a key will complete their original key issued form which will contain as a minimum:

- Keys will be returned to the Key Control Person upon the departure or reassignment of any person who was issued a key(s), and will not be given to any other individual for use or turn-in;
- Any person returning a key will complete their original key issued form which will contain as a minimum:
    1. The printed name and signature of person returning the key(s) and date;
    2. The printed name and signature of key control person receiving key(s) and date;
    3. Identification code of key(s) returned; and
    4. Identification of serial number(s) of key(s).
- Any employee issued official keys on a temporary basis shall promptly return them as ensured by the Key Control Person.

7.2.13 Loss/Damage/Destruction of Keys (Key Replacement): When a key to a designated controlled or restricted area is lost, the locks to that area must be changed, depending on risk, as soon as possible as old locks remain exposed until replaced.

- Lost or stolen keys must be reported immediately to the Key Control Person;
- Anyone reporting a lost or stolen key must provide written documentation to the Key Control person. This will include; date, time, circumstances of the loss, any key identification and any action taken to retrieve the key;
- Locks shall be re-keyed in a timely manner and new keys issued when keys are lost or stolen; and
- If a master key is lost, every master lock must be replaced and, depending how the keying is done, new keys distributed to the key holders.

7.2.14 Documentation: Key and excess core inventory logs will be developed and maintained for a period of no less than one year after the life of the key system being used;

- The DoD Lock Program can be referenced for documentation guidance. See Section Chapter 7 Subsection 1, Locks and Keys, above.
- Key access logs will be developed and maintained for a period of one year;
- A key issued form will be developed and utilized for key(s) issue and turn in. The form will be maintained until the key(s) are returned and for a period of no less than one year after the key(s) are returned; and
- All keys and excess cores will be secured and annually inventoried and documented.

Chapter 8: Physical Security Program-Safes and Storage Equipment

8.1 Physical Protection and Storage of Materials

8.1.1 Many types of storage equipment are used to store sensitive information, controlled substances, valuable equipment, and negotiable documents or funds. Only equipment described in this section or specifically approved by the designated CCC Manager should be used to safeguard such material when required by regulation or a risk assessment justifies the additional protection.

8.1.2 Employees or others having custody of sensitive information or CCC property are responsible for its safeguarding and proper handling.

8.1.3 Security officers should assure that authorized equipment is utilized for the protection of sensitive information and property, and that employees are made aware of such requirements.

8.2 GSA-Approved Security Containers

8.2.1 Classes of ERS Approved Security Containers: Class 1/Class 2/Class 3/Class 4/Class 5/Class 6

- Class 1: The Class 1 security container is insulated for fire protection. The protection provided is:
    1. 30 man-minutes against surreptitious entry;
    2. 10 man-minutes against forced entry;
    3. 1 hour protection against fire damage to contents;
    4. 20 man hours against manipulation of the lock;
    5. 20 man hours against radiological attack.
- Class 2: The Class 2 security container is insulated for fire protection. The protection provided is:
    1. 20 man minutes against surreptitious entry;
    2. 1 hour protection against fire damage to contents;
    3. 5 man minutes against forced entry;
    4. 20 man hours against manipulation of the lock;
    5. 20 man hours against radiological attack.
- Class 3: The Class 3 is an insulated security container, and the protection provided is:
    1. 20 man minutes against surreptitious entry;
    2. 20 man hours against manipulation of the lock;
    3. 20 man hours against radiological attack;
    4. No forded entry requirement.
- Class 4: The Class 4 is an uninsulated security container, and the protection provided is:

1. 20 man-minutes against surreptitious entry;
2. 5 man-minutes against forced entry;
3. 20 man-hours against manipulation of the lock;
4. 20 man-hours against radiological attack;

- Class 5: The Class 5 is an uninsulated security container, and the protection provided is:
    1. 20 man-hours against surreptitious entry (increased from 30 man-minutes on containers produced after March 1991);
    2. 10 man-minutes against forced entry;
    3. 20 man-hours against manipulation of the lock;
    4. 20 man-hours against radiological attack;
    5. 30 man-minutes against covert entry
- Class 6: The Class 6 is an uninsulated security container, and the protection provided is:
    1. 20 man-hours against surreptitious entry (increased from 30 man-minutes on containers produced after March 1991);
    2. No forced entry test requirement;
    3. 20 man-hours against manipulation of the lock;
    4. 20 man-hours against radiological attack;
    5. 30 man-minutes against covert entry.

8.2.2 Models of ERS Approved Security Containers

- Security Filing Cabinets: A variety of security filing cabinets is manufactured in both Class 5 and Class 6 models. Security filing cabinets are available in single, two, four, and five drawers and in both letter size and legal-size models.
- Schedule I/II Controlled Substance Security Containers: Schedule I/II Controlled Substance Containers are manufactured in both Class 5 and Class 6 models. In addition, this container is also available with various drawers, adjustable shelves, and in a configuration to keep contents segregated.

8.2.3 Record Safes Designed for Fire Protection: A labeling service has been established by the Underwriter's Laboratory (UL) to define the level of fire protection each safe can be expected to provide. Prior to 1972, the UL designations used an alpha designation that was the same as Safe Manufacturers National Association (SMNA). Both the former UL and SMNA designations are listed below with the current equivalent UL designation

- Fire Resistant Safes: There are three classes of fire-resistant safes. All three classes must pass three tests - fire endurance, explosion, and impact. During the fire endurance test, the inside temperature of a safe cannot exceed 350° F at any time during the test. At the end of the test, all papers inside a safe must be entirely legible and uncharred.
    1. Class 350-4 Hours (Former UL and SMNA Classification ("A"): A specimen safe containing papers and records is placed in a testing furnace, and the temperature is raised through a standard curve until it is 2,000º at the end of four hours.
    2. Class 350-2 Hours (Former UL and SMNA Classification ("B"): A specimen safe containing papers and records is placed in a testing furnace and must withstand two hours of exposure to heat reaching 1,850°F.
    3. Class 350-1 Hour (Former UL and SMNA Classification ("C"): A specimen safe containing papers and records is placed in a testing furnace for a one-hour exposure to heat reaching 1,700°F.
- Insulated Filing Devices: Insulated filing devices afford considerably less protection for records than the three levels of fire-resistant containers discussed above. The thermocouple devices to measure interior heat during the tests are located in the center of the interior compartment, and the insulated filing devices are not drop tested. As it is possible to confuse the 350-1 Insulated Filing Device with the 350-1 Fire-Resistant Safe, the label should be carefully noted.
    1. Class 350-1 Hour (Former UL and SMNA Classification ("D"): A specimen-filing device is placed in a testing furnace and is heated to temperatures reaching 1,700°F, for one hour.

2. Class 350-1/2 Hour (Former UL and SMNA Classification ("E"): A specimen-filing device is heated for one-half hour to a temperature reaching 1,550°F in a test furnace.

- Insulated Record Containers: . Because information technology (IT) records, such as magnetic storage media, begin to deteriorate at 150° F with humidity levels of more than 85 percent, Fire-Resistant Safes and Insulated Filing Devices should not be used to protect these types of records. To meet this requirement, a container that has been described as a "safe within a safe" was designed. This container has a sealed inner insulated repository in which the IT material is stored and an outer safe protected by a heavy wall of insulation. This type of container has been designed to protect IT records against 150°F temperature and 85 percent humidity for the period specified. Insulated Record Containers are labeled by UL as follows:
    1. Insulated Record Container, Class 150-4 Hour;
    2. Insulated Record Container, Class 150-3 Hour;
    3. Insulated Record Container, Class 150-2 Hour;
    4. Insulated Record Container, Class 150-1 Hour.

8.2.4 Burglary-Resistant Safes: Containers designed for burglary protection are classified in accordance with test data and specifications that conform to requirements of the UL. Burglary-resistant equipment will resist an attack by tools, torch, or explosives in proportion to their construction specifications.

- UL Ratings: Safes undergo severe testing before receiving ratings from UL. The meaning of the various label designations resulting from the UL test are described below.
    1. TL-15 or TL-30: The TL-15 or TL-30 signifies a combination-locked steel container offering a limited degree of protection against expert burglary with common mechanical or electrical tools. The container must successfully resist entry for a networking time of 15 or 30 minutes.
    2. TRTL-30 or TRTL-60: The TRTL-30 or TRTL-60 signifies a combination-locked steel safe designed and tested to give protection

against 30 or 60 minutes of attack with common electrical and mechanical tools, cutting torches, and any combination of these techniques. A successful attack consists of opening the door or making a two-inch square hole entirely through the door or front face.

- Applications: Burglary resistant safes may be useful in establishing protection of valuable equipment, controlled substances, and negotiable documents or funds. The cost of any proposed container should always be compared with the protection required for the items being safeguarded. For example, it would be an unrealistic expenditure of funds to purchase a burglary-resistant safe for the sole purpose of storing a $50 petty-cash fund.

8.2.5 Repairing Security Containers:

- Individuals who repair or drill security containers, vault doors, and padlocks must be cleared for access to the highest level of sensitive information or material stored within the container or must be escorted and continuously watched while working on the container.
- Containers can be returned to their original state of security for storage up to same level by meeting the following conditions:
    1. Replace all damaged or altered parts;
    2. When a container is drilled adjacent to or through the dial ring, replace the lock with one of equal integrity. Repair the drilled hole with a tapered casehardened steel rod (dowel, drill bit, bearing) with a diameter and length slightly larger than the hole. When the rod is driven into the hole, a shallow recess should remain at each end of the rod that is no less than one-eighth inch and no more than three-sixteenths inch deep. This will permit a substantial weld on the inside and outside surfaces. The outside of the drawer head must then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts;
    3. Containers that have been drilled or repaired in a manner other than as described above cannot be restored to their original state of security

integrity. The "Test Certification Label" and the ERS-Approved Security Container label, if any, must be removed. The container must not be used for storing sensitive information, and a notice to this effect must be marked on the front of the container.

8.3 Maintaining Approved Security Containers

8.3.1 General maintenance on approved security containers is recommended every 5 years. A trained and certified locksmith should be retained to examine and service security containers with built-in combination locks. Containers used for the storage of sensitive materials will be examined and repaired only by a cleared locksmith or under the constant supervision of a cleared person.

Chapter 9: Physical Security Program-Access to Facilities/Identification

9.1 General

9.1.1 Policy: This chapter establishes the policy for access to CCC facilities, and limits the establishment of facility entry controls to those necessary for the safety of CCC employees and the protection of CCC property and patient information. A properly organized and administered personnel identification system constitutes an important part of the physical security program. Such a system identifies those who have a need to enter and leave an area and also detects unauthorized personnel who attempt to gain entry. Entry to most space under CCC or ERS control requires identification of personnel at all times. At those facilities where the local security procedures require identification to gain access, employees and contractors needing access to these CCC and ERS controlled buildings and facilities must display proper identification.

9.1.2 This standardized approach will address accessing CCC facilities utilizing identification card, cards, Photo Access Cards (PAC), other company passes and credentials, X-Ray, magnetometer, irradiation screening devices and admittance to CCC facilities.

9.2 Definitions

9.2.1 Magnetometer: An electronic device used specifically to search personnel for hidden metallic weapons (knives and guns) at entrances to airports, public schools, courthouses, and other guarded spaces. When used with access control equipment, they can perform two functions:

- Detect the presence of concealed metal objects;
- Determine the size of those objects.

1. Metal is detected by measuring the change in an established magnetic field when dense metal or ferrous materials are moved through the field. The antenna of a detector sets up a magnetic field around itself. As the antenna of the detector is brought near metal or metal is moved past the antenna, the pitch from a tone generator increases, thereby alerting the operator to the presence of metal. Measurement capabilities are adjustable allowing for varying the amount of metal desired to be detected.

9.2.2 Photo Access Card (PAC): A PAC is a physical artifact, a plastic card issued by CCC to employees and contractors, which allow the bearers, authorized access to CCC Facilities.

9.2.3 Visitor: Any person who is not a CCC employee, CCC patient or CCC contractor with current CCC background/suitability and issued a CCC Photo Access Card (PAC).

9.2.4 X-Ray System: A device or system that inspects the contents of a package or container for concealed explosives or contraband. Some systems can only detect objects made of materials possessing high atomic numbers, such as steel, tin, aluminum, and iron. Other systems can detect materials with both high and low atomic numbers. Some systems have two monitors, one for objects with high atomic numbers and one for objects with low atomic numbers. Color systems presently available use only one monitor to view both types of materials. Specific colors are assigned to high and low atomic number materials.

9.4 General

9.4.1 Entry control facilities provide the first public impression of CCC. They will present the proper appearance for visitors, employees, and CCC personnel. The layout, landscaping, and architecture of the facilities are factors in this image. The architectural design of the facilities will comply with CCC's architectural design standards.

9.5 Responsibilities

9.5.1 The Director of the Security will ensure that all persons entering and exiting any CCC facility will adhere to access and egress procedures established in this handbook.

- Employees of CCC:
- All CCC employees and contractors (including guards, maintenance, and cleaners) will complete a favorable suitability-to-be-authorized and issued a CCC identification prior to entering and/or performing any authorized work in a CCC owned or leased facility:
- The Contract Security Firm/ERS will conduct federal, state and local criminal and warrant checks on cleaning force personnel and answering service employees;
- New cleaning personnel and answering service employees must be checked prior to their utilization;
- All names should be rechecked annually;
- Cleaning personnel or answering service employees are to provide photo identification each time they enter the premises to perform their duties; and
- CCC will issue standardized contractor PACs.

9.5.2 Photo Access Card Identification Carriers:

- Maintain control of the issued photo access card (PAC) identification.
- Safeguarding the photo access card (PAC) identification badge from loss or misuse,
- Immediately report any lost or stolen photo access card identification badge; and
- Notify his/her supervisor in writing of the circumstances surrounding the lost/stolen badge or credential. Follow ERS guidelines to report a lost/ stolen badge.

9.5.3 Employees who have lost or forgotten their photo access card (PAC) identification or other issued CCC facilities issued access badge will be issued visitors identification after that employee has been verified as employed by CCC;

9.5.4 Photo access card (PAC) identification will be relinquished by all employees, who shall, prior to resignation, termination; retirement, transfer etc., return the CCC Photo Access Card (PAC) identification badge or other issued CCC facilities issued access badge.

9.5.5 The Designated Manager will:

- Ensure compliance with minimum CCC security requirements as determined by the Program Head and/or designee;
- Establish additional protection requirements for facilities and space under their control as long as these procedures conform to the policy established by this chapter;
- Develop and implement adequate procedures to protect CCC employees and property;
- Determine normal working hours and non-working hours for the facility;
- Determine if special access controls to the facility are necessary during normal working and non-working hours, and if they are necessary, establish only the minimum controls required;
- Coordinate and establish these special access controls and other protection requirements with ERS if the building is operated or leased by CCC; and
- The Designated Manager or Security Liaison will determine if it is necessary to establish additional access controls to the facility during normal working hours:
    1. Access controls may be enhanced if the Designated Manager or Security Liaison determines that there is a threat to harm employees, to steal CCC property, or to gain unlawful access to information which is protected against unauthorized access by federal, state, or local rules or regulations.

9.5.6 Designated Managers and Security Liaisons are responsible to ensure that the physical security policies and procedures applicable to individual program activities are adhered to by all employees.

9.5.7 Designated Managers or Security Liaison of a CCC owned facility establish and maintain physical security, predicated on programmatic requirements, if any, to protect:

- CCC property;
- Records; and
- The well-being of CCC employees.

9.5.8 Designated Managers or security officer of both CCC-owned and CCC-leased space, ensure staff compliance with all applicable policies and procedures in safeguarding and protecting:

- CCC personal property;
- CBD or Medical Marijuana products (if applicable);
- CCC records (personnel, sensitive documents, etc.); and
- ADP security requirements.

9.6 Access Controls

9.6.1 The Program Head or designee determines the necessary access controls and systems for all CCC facilities based on the requirements set forth in this handbook. Planning is required to include:

- Establishment of a system for positive identification of personnel and equipment authorized to enter and exit the facilities; and
- Maintenance of adequate physical barriers that will be deployed to control the facilities.

9.6.2 The number of entrances will be kept to a minimum as each entrance must be controlled:

- VSS will provide surveillance of all access control operations to include the access control area, vehicle search areas, final denial barriers, and pedestrian access points.

9.6.3 The Director of Security official is responsible for oversight and administration of the badge program if applicable. Personnel and equipment must be provided to properly administer a badge system.

- Planning will also include increasing vigilance and access restrictions during periods of activity that potentially increase the threat.

9.6.4 Public access control (PAC) points and entry control facilities (ECF) act as a monitoring and clearance areas ensuring the proper level of access control for all personnel, visitors, and commercial traffic. The objective of a PAC and ECF is to ensure:

- Only authorized personnel and/or vehicles have access to specific facilities and/ or areas;
- A level of protection from unauthorized access is provided; and

- Interception of contraband, such as weapons, explosives, drugs, classified material, etc.

9.6.5 Public access areas are areas within the building where services are provided to the general public:

- Uncleared persons may enter these areas without escort but will be properly screened prior to admittance;
- The public access control area (normally in the main entrance lobby of the building) will provide for screening of visitors and employees before admittance into CCC controlled areas/space; and
- The public access control operations can consist of a screening area, a walk-through metal detector (WTMD) or hand-held metal detector (HHMD), a guard, controlled doors, a controller, and/or a security receptionist.

9.6.6 All forms of issued CCC identification are the property of CCC and may be retrieved at any time by the issuing manager or contract security authority for just cause including, but not limited to:

- Any unauthorized use, including use for other than official or authorized purposes;
- Altering the badge/card or pass in any manner from original issued condition;
- Repeated loss; and
- Failure to display while in facility.

9.7 CCC-Operated or Leased Facilities

9.7.1 The Program Head or designee in conjunction with the Director of Security will determine the normal level of protection necessary to control entry to CCC-operated facilities. If access controls during normal working hours are necessary according to the policy of this order; the access procedures will be developed in conjunction with the contract security firm/ERS.

- ERS will recommend the security hours access control procedures in conjunction with the Designated Manager.

9.7.2 The FPS is responsible for providing facility perimeter physical security predicated on programmatic needs at all facilities leased to Federal agencies.

9.7.3 Specific information and details pertaining to the administration of security in each of these discrete security areas should be included in the Site Security Plan/Program.

- General Services Administration's (GSA) responsibilities for the protection of life and property in federally owned and leased buildings and the responsibilities of those occupying these facilities;
- Except as otherwise ordered, property shall be closed to the public after normal working hours. During normal working hours, property shall be closed to the public only in emergency situations when reasonably necessary to ensure the orderly conduct of CCC business. The decision to close a property shall be made by the designated official under the facility site security plan/program;
- For buildings and grounds for which the GSA has space assignment responsibility, GSA will furnish as normal protection not less than the degree of protection provided by commercial building operators of similar space for normal risk occupants, as determined by GSA; and
- Occupants of GSA assigned space shall cooperate to the fullest extent possible with all pertinent facility regulations and procedures, and shall make recommendations for improving protection.

9.8 Non-CCC Owned or Leased Facilities

9.8.1 When CCC elements occupy facilities not under CCC control, the Program Head will determine if access control procedures are in accordance with the policy of this chapter.

9.8.2 Dissemination of Access Control Information: When access controls are implemented, the Designated Manager will:

- Publicize access control procedures to all facility occupants;
- Make procedures available at each access control point for review by those wishing access to the facility;
- Provide written access control procedures to each guard post or receptionist, defining responsibilities and procedures; and

- Install signs at all facility entrances announcing that access to the facility is controlled.

9.9 Photo Access Cards (PAC)

9.9.1 The PAC should be kept in a safe place which is convenient enough to ensure that it will be brought to work. A good rule of thumb is to afford the PAC the same protection given to credit cards. DO NOT write Personal Identification Numbers on the PAC.

9.9.2 The CCC Photo Access Card (PAC), identification badge, or other CCC facilities issued access card is not for official identification and will never be used outside of a CCC facility for the purpose of personal identification.

9.9.3 Blank stock of any CCC PACs will be secured in a locked container and remain under the positive control of the issuing manager.

9.9.4 Each issuing official will maintain detailed accountability records of all PACs, to include:

- Issuance;
- Returns;
- Loss;
- Destruction;
- Unused stock on hand; and
- Confirmation of suitability.

9.9.5 Destroying CCC PACs

- All CCC PACs will be returned to the issuing office for destruction;
- All issuing offices are responsible to develop destruction control processes which will include as a minimum:
- Maintain log with card holder's name, card number and date returned and date destroyed;
- Destruction logs will be maintained for a period of no less than 5 years;

- All identification pass/badges will be destroyed by shredding, utilizing an ERS approved shredder

9.10 Visitors

9.10.1 Control of the internal movements of personnel within a facility is necessary to ensure that only authorized persons are permitted in secured areas and that visitors do not wander through the facility unescorted. Accordingly, during business hours, CCC facilities are normally open to visitors and only restricted to authorized individuals after business hours.

9.10.2 All visitors will be issued a visitor's badge/card or pass for the purpose of escorted or unescorted authorization to visit in a CCC controlled facility/space/area. Each facility will establish an internal Visitor Control procedures and criteria for visitor badging and maintain positive control of all visitors, as a minimum:

- A unique visitor's temporary or hard badge/card or pass will be developed indicating:
    1. Name of facility;
    2. Visitor badge/card or pass number; and
    3. Visitor escort or unescorted status.
- Visitor badge/card will be strictly controlled and inventoried;
- Visitor badge/card issuance shall not exceed 12 hours;
- Visitor's logs will be maintained indicating, as a minimum:
    1. Visitors' time in and time out;
    2. Visitor's full name printed and their signature;
    3. Visitor's government-issued photo ID source for identification purpose;
    4. Visitor's company/organization and contact number;
    5. Visitor badge/card or pass number;
    6. Sponsor's full name printed and their signature; and
    7. Sponsor's contact number.

9.10.3 The CCC Visitor's identification badge/card or pass will be used for identification purposes only within CCC facilities where it was issued. A visitor badge/card or passes is required and the type utilized is based on the need of the facility and at the discretion of the Program Head or designee to facilitate the entrance of employees and visitors requiring access into a CCC facility/space or area when the visitor is not authorized to receive of a Photo Access Card (PAC) identification badge.

- Types of visitors badges/cards or passes
    1. Disposable badge/card or pass;
    2. Hard badge/card or pass;
    3. Unescorted badge/card or pass; and
    4. Escort required badge/card or pass
- Persons who may require a visitor badge/card or pass may include, but are not limited to:
    1. Employees;
    2. Visitors;
    3. Construction workers;
    4. Maintenance workers;
    5. Vendors; and
    6. Friends, family.

9.10.4 If a disposable visitor badge/card or pass is issued, issuance will be maintained either by manual or electronic means:

- The badge/card or pass will have as a minimum the visitor's full name and date of expiration;
- Identify visitor as requiring escort or unescorted status; and
- Can be issued to employees who have lost or forgotten their CCC Photo Access Card (PAC) identification badge or other CCC facilities-issued access badge:
    1. The Security Liaison will verify the individual in the CCC Personnel Security Data Base or with Director of Security;
    2. Missing badge/card or pass (possibly due to loss or theft) must be immediately reported to the Security Liaison.

9.10.5 If a visitor's hard badge/card or pass is used, a strict accounting of the issuance will be maintained either by manual or electronic means and the visitor procedures will include an exchange process for issuance for a piece of photographic government-issued identification.

9.10.6 Visitors are responsible for safeguarding their visitor's identification badge/card or pass from loss or misuse.

9.10.7 Lost or stolen visitor identification badges/cards/passes:

9.10.8 The Security Liaison will:

- Maintain documented records of lost visitor badges/cards or passes;
- Complete a re-issuance of visitor badges/cards or passes when the number of badges lost exceeds ten percent of the overall number of badges issued:
- If re-issuance is accomplished all obsolete badges/cards or passes will be destroyed and a destruction documented.

9.10.9 Visitor identification badges are only issued for the purpose of authorizing a visitor into a CCC facility, area or space for the purpose of meetings, briefs, etc or vendors supporting CCC activities.

9.10.10 Individuals denied a PAC based on suitability are not authorized access;

9.10.11 This includes short term visitor access.

9.11 Escorts

9.11.1 All CCC employees and contractors assigned escort responsibilities will have a valid CCC Photo Access Card (PAC) identification badge or other issued CCC facilities issued access badge and authorized entry into the areas in which they are performing escort duties.

9.11.2 All CCC employees and contractors assigned escort duties are responsible to:

- Ensure visitors under escort have been properly screened and badged;
- Not escort more than four (4) visitors at one time;
- Ensure escorted visitors are under visual contact and positive control at all times;
- Ensure escorted visitors return visitor identification upon departure;
- Report any unauthorized activities by escorted visitors to the Security Liaison;
- Never leave escorted required visitors unattended;
- Never escort a visitor into a restricted, controlled or sensitive area unless prior approval has been granted by the Security Liaison; and
- Ensure visitors are aware of visitor identification safe keeping including:
    1. Report of loss of identification to sponsor;
    2. Proper display; and
    3. Return policy.

9.12 Visitor Parking

9.12.1 Where the facility is operated and managed by CCC the following will apply:

- No unauthorized direct access into any facility from a parking lot or parking structure by visitors;
- Visitor spaces are not intended to accommodate the daily or personal needs of employees who work in or near the CCC facility;
- Post signage and arrange for towing unauthorized vehicles:
- Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.
- Spaces will be designated for the exclusive use of visitors and handicap persons;
- Utilize effective lighting to provide added safety and deter illegal or threatening activities;
- Twenty-four hour VSS surveillance and recording is required at all locations as a deterrent:
- Requirements will depend on assessment of the security level for each facility.

- Digital video recordings (DVR) are also highly valuable as a source of evidence and investigative leads; and

9.13 Electronic Access Controls

9.13.1 For detailed information on access controls see Appendix (CCTV) and Appendix (IDS).

9.13.2 Plan for locking devices or controls at perimeter and interior doors, providing effective key control. Plan for protection; cleaning, and maintenance personnel and determine hours, locations, and levels of access for such personnel.

9.13.3 Vehicles and Traffic Control. If public vehicle entrances have gates, they will be electronically opened and closed.

- Accommodations for handicapped visitors will be provided.

9.13.4 Vehicle entrances with restricted access at facilities associated with a high threat level will be equipped with electrical or hydraulic vehicle gates or movable barriers.

- Vehicle barriers may be controlled by: (See Appendix 3: Perimeter Security Barriers for more detailed information).
    1. Card readers;
    2. Biometric devices;
    3. Proximity tags;
    4. Electronic keypads;
    5. Remotely by line-of-sight or using VSS; or
    6. For high traffic areas, one-way entry and exit lanes shall be created.

9.13.5 Access control systems will be provided at perimeter doors, public waiting and information areas, visitation areas, processing areas, sally ports, secure vestibule, loading docks, and entrances to restricted areas.

9.13.6 A personnel-based access control system relies on a person to:

- Positively identify individuals requesting access;
- Determine if the access is authorized; and

- Secure the access port ensuring only the individual(s) authorized have gained access.

9.13.7 Access Control Systems may be in the form of stand-alone, one or two door units, small networks for 8-16 doors, or larger multi-door, multi-tasking systems. Characteristics of this type of system are:

- All authorized users are provided with unique pass cards, tags or personal identification numbers (PINs);
- Audit trails are available;
- Electrical power is required at each control point;
- Individual users can be deleted from the system without the need to recover cards, tags, pins or keys; and
- These types of systems are ideal for areas with 25 or more users and large systems controlling interior and exterior access control readers.

9.14 Screening Procedures

9.14.1 Entry security must follow procedures as dictated by the Program Head that may include:

- A visitor control/screening system, acceptable to the CCC, is required. At a minimum, the system shall require Security Guards/Receptionist to screen visitors;
- Security Guards for public lobbies and public entrances shall be required for such purposes as:
    1. ID/pass control;
    2. Manning X-ray and magnetometer equipment.
- Guards can be furnished via either:
    1. Lessor-furnished operating agreement or
    2. Full leasehold control methods.
- If guards are lessor-furnished, they shall be trained and licensed in accordance with CCC standards prescribed in this handbook;
- Guards manning magnetometers and X-ray equipment may be armed as determined by CCC; and
    1. Guards will direct the building population and visitors through the magnetometers.

2. See Appendix 9.14, Screening Procedures, for more information.

9.14.2 Facility Security Standards:

- X-ray and magnetometer screening devices at all public entrances for the screening of visitors, contractors, etc., and all of their purses, bags, briefcases, packages, etc. if determined a need by the Program Head
- X-raying of all packages entering the building delivered by contractors, couriers, etc., as determined a need by the Program Head.

9.14.3 Mail and packages entering the building will be:

- Subject to X-ray screening when appropriate;
- Visual inspection by Security Guards:
    1. Packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from CCC property, are subject to inspection.
    2. Security Officers may divert large truck shipments to a secondary location for screening purposes; and
    3. CCC reserves the right to negotiate security enhancements necessary for securing any unsecured block of space with a separate entrance (e.g., ground floor retail) based on a ERS Building Security Assessment.

9.14.4 Visitor screening procedures will be developed by the Program Head or designee. The procedures will:

1. Consider the building design;
2. Rate and flow of visitors;
3. Threat level;
4. Personnel available; and
5. Types of technical equipment installed.

- Screening procedures will:
    1. Maintain maximum desired security;
    2. Provide access only to persons with legitimate need.

9.14.5 The use of walk-through metal detectors (WTMD) or hand-held metal detectors (HHMD), people-control barricades, and door controls can be incorporated into the facility access procedure. The procedure will include:

- Provisions for active inspection and thorough visual checks of the contents of all packages, briefcases, handbags and similar items; such packages that may be transported by:
    1. A visitor requesting access;
    2. A freight carrier;
    3. An express package delivery firm;
    4. The U.S. Postal Service; and
    5. U.S./Pennsylvania Government courier.
- Visual checks of carried items including passage utilizing a WTMD or inspection using a HHMD before allowing access into any CCC space.

9.14.6 Additional:

- Emergency power sources to critical systems (alarm systems, radio communications, computer facilities, VSS monitoring, fire detection, entry control devices, etc) are required

9.15 Prohibited Entry Notice

9.15.1 The authority of a CCC Designated Manager or Security Officer to take reasonable, necessary and lawful measures to maintain law and order and to protect personnel and property shall include the authority to issue a Prohibited Entry Notice:

- That authority also includes the removal from or the denial of access to, any CCC facility, site or space of individuals who threaten the orderly administration of the site;
- That authority must not be exercised in an arbitrary, capricious, or discriminatory manner; and
- Removal or denial actions must be based on reasonable grounds and be judiciously applied.

9.15.2 Pennsylvania law states that all persons entering in or on CCC property are prohibited from loitering, exhibiting disorderly conduct, or exhibiting other conduct on property that:

1. Creates loud or unusual noise or a nuisance;
2. Unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways or parking lots;
3. Otherwise impedes or disrupts the performance of duties by CCC employees; or
4. Prevents the public from obtaining CCC's services provided on the property in a timely manner.

9.16 Prohibited Items

9.16.1 Prohibited Articles: The following articles are prohibited from CCC facilities, unless approved by the designated Security Contractor/local authority for security:

- Any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property;
- Sites shall, at a minimum, employ administrative procedures to deter the introduction of explosives into facilities.

9.16.2 Leases shall state that CCC reserves the right to post applicable CCC rules and regulations at each public entrance in a CCC-occupied facility for such things as, but not limited to, barring the unauthorized possession of firearms and dangerous weapons.

9.16.3 Controlled Articles: The following privately owned articles are not permitted/ authorized in CCC facilities without prior written authorization from the Program Head or designee:

- Recording equipment (audio, video, optical, or data);
- Electronic equipment with a data exchange port capable of being connected to automated information system equipment (portable computer drives or other data storage devices);
- Radio frequency transmitting equipment; and
- Computers and associated media.

9.16.4 Controlled Substances (e.g., illegal drugs and associated paraphernalia, but not prescription medicine) are not permitted/authorized.

9.16.5 Other items prohibited by law: Alcoholic Beverages.

9.17 Signage

9.17.1 Interior and exterior signage is standardized by function; Information, Direction, Identification and Regulation and is required at all PA business facilities. All signage shall follow the standards prescribed by the Commonwealth of PA.

9.17.2 A well-designed site should use as few signs as possible. Signs should make the site clear to the first-time user by identifying multiple site entrances, parking and the main building entrance.

9.17.3 Conformity of signage and directions:

9.17.4 Signage should be clear to avoid confusion and direct users to their destination efficiently. If an escort service is available, signs should inform users; and

9.17.5 Generally, graphics and style of site signage should be in keeping with the signage used inside the building. Signs integrated with architectural elements can also be very effective. There shall be a consistency in the font style and color plus any directional symbology used in site and building signage. Signage placement can be an important detail element of the building design whether prominently displayed and tooled into the exterior building wall materials or as a freestanding component near the entrance to the facility.

9.17.6 Persons in and on property shall at all times comply with signs of a prohibitory, regulatory, or directory nature and with the lawful direction of Security Officers and other authorized individuals.

9.18 Security Violations

9.18.1 Violation of these procedures constitutes a security violation; the Security Officer will comply with all required actions.

10.1 Contract Guard Services

10.1.1 A guard force is an effective and useful component of a facility's physical security program. The effectiveness of alarm devices, physical barriers, and intrusion detectors depends ultimately on a response by a skilled guard force. Guard services can be provided by ERS, a private company under contract to ERS or CCC, or employees of CCC.

10.2.2 Criteria for Determining Need: As cited in Appendix B, "ERS Facility Security Standards," evaluates a facility for security guard requirements to include a security guard patrol. The number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors. Guard services are recommended under, but are not limited to, the following circumstances.

- At facilities to meet visitor control and screening requirements;
- The mission of the facility is particularly critical;
- There is a high level of sensitivity of information handled at the facility, e.g., HIPAA and patient information;
- An in-house response capability is needed, e.g., the facility contains alarmed vaults or other sensitive operations, and off-site guards or police are not close enough for quick response;
- The facility is vulnerable to theft or damage, e.g. a facility location in a high crime area;
- Pedestrian or automobile traffic is heavy or congested and requires special controls.

10.2.3 Cost Factors: As with any expenditure of funds for security, the annual costs of guard services normally should not exceed the monetary value of the protected items.

- A substantial expense for guard services may be required for crowd or traffic control, for safeguarding sensitive information, or for protecting material or functions which have high intrinsic rather than monetary value. This is especially true as applied to the safety of employees since it is impossible to put a dollar value on human lives or peace of mind. A guard post in a high crime area may yield substantial benefits in terms of improved safety, higher employee morale, increased productivity, and a better image of CCC.

10.2.4 Guard Duties: In making a decision about whether to utilize a guard force of any size, consider the following duties that guards may properly perform:

- Entrance Control: Operate and enforce a system of access control, including inspection of identification and packages.
- Roving Patrol: Patrol routes or designated areas, such as perimeters, buildings, vaults, and public areas.
- Traffic Control: Direct traffic (vehicular and pedestrian), control parking, check permits, and issue citations.
- Key Control: Receive, issue, and account for certain keys to the building and its internal areas.
- Security and Fire Systems: Monitor, operate, and respond to intrusion and fire alarm systems or protective devices.
- Utility Systems: Monitor, record data, or perform minor operations for building utility systems.
- Lost and Found: Receive, receipt for, and store found items.
- Flying of the United States Flag: Observe flag flying procedures.
- Reports and Records: Prepare reports on accidents, fires, thefts, and other building incidents.
- Response to Emergencies: In case of any emergency, such as fire, bomb threat, assault or civil disturbance, respond, summon assistance, administer first aid, and assist public safety personnel.
- Law and Order: Maintain law and order within the area of assignment.

- Hazardous Conditions: Report potentially hazardous conditions and items in need of repair.

10.2.5 Personnel Requirements:

- Manpower: The number of full-time guard posts for a facility is determined by the Program Head and the site manager. The decision should be based on a comprehensive ERS physical security survey such as described in this handbook. The number of guard posts will be determined by the local crime rate, number of entrances, alarm systems to respond to, and other factors peculiar to each facility. The Program Head must calculate the total number of posts and hours of coverage. The bidding contractor will be responsible for calculating the total number of guards required, taking into account the number and duration of shifts, reliefs, sick leave, and other administrative factors.
    1. Armed Guards: Guards operating magnetometer and X-ray screening devices are required to be armed in order for the guards to appropriately respond to all possible threats and volatile situations. If guards are armed for a deterrent effect, i.e., to prevent crime or other unauthorized activity, responsible officials must weigh that advantage against such disadvantages as the danger to innocent personnel if a firearm is used by a guard; the possibility of an accidental discharge; and the possibility, no matter how remote, of irrational behavior on the part of a guard in a weak moment or under pressure.
    2. Firearms may be used only defensively, and only for the protection of life and property.
    3. When making a decision as to whether guards at a facility should be armed, the Program Head and the Director of Security should give strong consideration to the factors below. If contracting, every possible effort should be made to include requirements in the contract Statement of Work that will task the contractor with providing properly selected and trained personnel and maintaining appropriate performance and conduct standards. These factors apply whether hiring guards directly or dealing with a contractor.

- Firearms training, including judgment shooting and firearms safety.
- Knowledge of criminal activities and proper law enforcement response procedures.
- Judgment and emotional stability.
- Experience and demonstrated ability to retain composure under pressure.
- A personal history free of arrests or other criminal activity.

10.2.6 Supervision: Supervision is required for all guard posts and is usually requested at a ratio of one hour of supervision for each eight productive hours on post.

- On small contracts with three or fewer posts or at isolated sites, the use of roving supervisors may be the only practical or cost-effective method of supervising the contract.
- At sites where there will be eight or more posts, an on-site supervisor should be required, at least during the hours of heaviest traffic and greatest productive hours on posts. After-hours supervision can be performed at the one to eight ratio by roving supervisors. Large forces and facilities generally require more supervision; a contract with thirty or more shifts per week should have full-time supervision.

10.2.7 Statement of Work (SOW) for Guard Services: After the decision has been made to contract for guard services and the nature and extent of required guard services has been determined, the Director of Security develops a Statement of Work (SOW), which describes the contract effort required. The SOW will usually contain the following elements:

- Scope of Work: A general description of the contract, e.g., guard services, the premises, and the management and equipment required.
- Contract Effort Required: . A detailed description of productive man-hours and supervisory man-hours.
- Services Required: Basic duties of guards, by post, and work scheduling procedures, i.e., nature of coverage and duration of shift and relief assignments.

- Supervision: Duties of project manager, on-site supervisor, and key contract personnel.
- Authority and Jurisdiction: Permits and licenses required, weapons permits, bonding, and liability.
- Use of Force Policy: . Include a "use of force" policy in your Statement of Work. For a sample, contact the Security Management Office.
- Regulations and Procedures: Procedures for protection, including the following:
    1. Officer Duty Book: A separate loose-leaf binder containing the complete duty instruction for all posts involved, to include instruction for emergency procedures.
    2. Contractor Guard Information Manual: This handbook contains the course of instruction, which the contractor must teach to contract guards.
- Equipment/Uniforms/Materials:
    1. Items to be furnished by the CCC, such as electrical and mechanical equipment, furniture, safes and weapons cabinets, telephones, computers, lockers, building utilities, and books and supplies.
    2. Items Furnished by the Contractor:
        - Uniforms, insignia, and accessories.
        - Supplementary equipment including flashlights, batons, belts, whistles, notebooks, and safety and inclement weather apparel.
        - Radios, including frequencies, permits and licenses, base stations, and performance specifications for the site.
        - Firearms, including permits and licenses, holsters and ammunition, issuance and control procedures and records, storage cabinets, loading/unloading instructions and safety procedures, and training and certification requirements.
        - Motorized patrol vehicles.

10.2.8 Qualification of Personnel: To be eligible to perform under a guard services contract, each contract guard should satisfy the following education, experience, and medical requirements:

- Possess a high school diploma or equivalency and have two years of experience demonstrating:
    1. The ability to meet and deal with the general public (and speak the English language fluently);
    2. The ability to read, understand, and apply printed rules, detailed orders, instructions, and training materials;
    3. The ability to maintain poise and self-control under stress;
    4. The ability to construct and write clear, concise, accurate, and detailed reports; and
- When armed, proficiency in the use and safe handling of a Glock .40 caliber handgun or Glock 9mm handgun.
- Contractor employees should be well proportioned in height and weight, and in good general health without physical or mental disabilities that would interfere with the performance of their duties.
- Physical fitness should be evidenced on a ERS-78, Certificate of Medical Examination, by a medical examination administered by a licensed physician. The medical examination should indicate that guards have:
    1. Freedom from serious illness or communicable disease;
    2. Binocular vision, correctable to 20/20 and not be color blind;
    3. Hearing within normal speech range and volume; and
    4. Unimpaired use of hands, arms, legs, and feet and ability to run, lift, and climb stairs.

10.2.9 Suitability Requirements: The contract should contain suitability standards and instructions regarding forms to be submitted and procedures for processing and providing suitability determinations.

- For contracts where no security clearance is required, background checks conducted by ERS should be used in accordance with the provisions contained in this handbook.
- If a security clearance is required, the suitability processing shall be covered in the Statement of Work.

10.2.10 Special Requirements for Supervisors: Supervisors must be individuals of unquestionable integrity who have demonstrated exceptional qualities of maturity and judgment, with at least two years of field experience in supervision.

10.2.11 Training: The contract should specify in detail training to be provided by the contractor to its employees, to include the following:

- General duties, such as conduct, appearance, use of radios and equipment, first aid, and emergency duties.
- Physical protection, such as crime prevention, patrol techniques, and responses to alarms.
- Enforcement, such as laws and regulations, search and arrest techniques, and preservation of evidence.
- Special problems, such as bomb threats and searches, hostage situations, or civil disturbances.
- Crimes, including criminal and civil law, burglary, robbery, arson, and responses to crimes in progress.
- Firearms, including safety, judgment shooting, and a detailed specification of qualification standards to be met. The contractor is responsible for obtaining all required training and certifications.
- Special training for supervisors in addition to basic training should include techniques for issuing written and verbal orders, uniform clothing and grooming standards, post inspection procedures, and employee motivation.
- Special requirements of the facility, such as operation of access control systems, special response procedures for sensitive areas, and the emergency evacuation plan.

10.2.12 Reporting to Work: The contract should specify in detail the procedures for recording and verifying the contractor's hours of work and a schedule of penalties or deductions for failure to perform the required work.

10.2.13 Removal from Duty: The contract should include the CCC's authority to request the immediate removal of any contract employee from the work site upon a determination that the individual has been disqualified for suitability or security reasons, or who is found to be unfit for performing security duties.

10.3 Guard Force Orders

10.3.1 Guard force orders are instruction to the guard force. They are to be developed by the Director of Security. They should be reviewed by the project manager and/or site supervisor for concurrence or suggested revisions. The orders should be reviewed quarterly to be certain that they remain complete and correct.

10.3.2 There are three types of guard force orders: general orders, post orders, and special orders:

- General orders specify policies, procedures, and other basic information that applies to all posts.
- Post orders list the particular duties at each individual post.
- Special orders are short term or limited-scope instructions, which cover special subjects such as temporary posts, special event coverage, and unusual or non-recurring duties.

10.4 Guard Force Management

10.4.1 Guard Force Management: Successful operation of a guard contract requires constant and careful supervision to assure that all aspects of the contract continue to run smoothly. After initial negotiations to procure the contracted services, the Program Head should perform the following services on a continuing basis:

- Maintain liaison with local police officials;
- Monitor the performance of supervisors to assure that post assignments are timely and efficiently made, that time sheets are kept accurately, that property is being accounted for, that post orders are up to date and properly distributed and read, and that all provisions of the contract are being met.
- Monitor the contractor's compliance with contract requirements for training of employees including weapons training, special facility or facility systems and

unique requirements, and for guards to carry the proper identification and certification of training.

- Monitor the performance of all guards on posts, including roving patrols, to assure coverage of all alarmed areas and other sensitive features of the facility, and to assure emergency response procedures are followed swiftly and accurately.
- Assess penalties for non-performance or shortcomings in the contract, such as discrepancies in claimed hours of service, services not performed or posts not manned, guards sleeping, eating, or misbehaving on posts, etc.

11.2 Currency/Funds

11.2.1 General: If a CCC office should have cash on hand, the Program Head recommends that the storage requirements below for small and large funds be established.

11.2.2 Storage Requirements for Small Funds: Safekeeping facilities should be tailored to the size of the fund, as well as the vulnerability of the facility. Relatively small funds ($500 or less) may be stored in a UL rated burglary-resistant safe offering a limited degree of protection against expert burglary with common mechanical or electrical tools. Also, security containers equipped with built-in combination locks are approved for the safekeeping of CCC funds. The cost of any proposed container should be compared with the amount of cash being safeguarded.

11.2.3 Storage Requirements for Large Funds. Because they provide adequate forced entry protection, either an Approved Class 5 security container or an UL-rated burglary resistant safe should be utilized to safeguard large funds. Based upon local vulnerabilities, consider installation of a panic or holdup alarm. The cost of any additional security systems should be compared with the amount of cash being safeguarded.

11.2.4 Other Security Considerations:

- When possible, locate any cash-handling operation or facility on an upper floor, as deep as practical within a building. This will preclude easy access from the street and may hamper a criminal's opportunities for getting away easily.
- Take reasonable precautions to safeguard CCC funds. For example, screen the handling of funds from public view to the extent practical. Rather than holding large amounts of cash, obtain advances in the form of several checks to be cashed only as needed. Avoid attracting attention when performing sizable cash transfers by doing so in an inconspicuous and non-routine manner.
- Request escort from the guard service or local law enforcement to move large amounts of funds between the fund activity and depositories. An even higher degree of safety can be achieved by using electronic funds transfers to the maximum extent practicable.
- Limit the number of employees allowed access to the storage container and the lock combination. Consider procedures to record each time the container is opened and closed, by whom, and a closing witness check.
- Prepare emergency procedures to follow in event of a holdup or other critical situation. Coordinate emergency procedures and response planning with local law enforcement officials.

11.4 Office and Laboratory Equipment

11.4.1 General: These guidelines are provided to assist security officers and custodial property officers in establishing appropriate physical security measures necessary to protect office and laboratory equipment. Office equipment includes office automation equipment, microcomputers, computer terminals, calculators, audiovisual equipment, telephone, facsimile machines, etc. Laboratory equipment includes the wide variety of scientific instruments used by CCC.

- Because of the variety of work places where such office or laboratory equipment is found, it is not appropriate to establish mandatory physical protection requirements for all environments. Security officers and responsible custodial property officers must determine the level of security needed, based on an

assessment of threats to the equipment, including a review of past incidents of theft and vandalism in the office/laboratory, building, and surrounding area.

11.4.2 Threat Determination:

- Data indicates that valuable and portable office and laboratory equipment are most commonly stolen or vandalized by semiskilled and unskilled burglars, employees or visitors. However, the security measures mentioned here may also apply against other illegal or unauthorized acts. For example, a lockable cabinet that protects a computer against theft also helps prevent unauthorized use of the equipment.
- During security evaluations, the security officer or responsible custodial property officer should look at the building and interior areas, taking into consideration:
    1. What items are most likely to be stolen?
    2. How could entry be gained?
    3. Where could property be concealed for later removal?
    4. Can exit with property be easily accomplished unchallenged?
    5. Has the activity experienced equipment thefts during business and after business hours?
- Special Security Considerations: In addition to the various protection measures discussed in detail elsewhere in this handbook, consideration should be given to provide additional protection to portable equipment. The security measures listed below will increase the time required to tamper with or remove the equipment.
    1. Unoccupied offices and laboratories should be locked, especially after business hours.
    2. Lock small and valuable equipment in a cabinet or closet.
    3. Maintain tight control and accountability of keys, and keep keys in a secure place.
    4. Do not store unused equipment in isolated areas.
    5. Escort wandering or "lost" visitors to the right office.
    6. Establish a system to ensure that the last person to leave at night checks that all windows and doors are closed and locked.

7. Ensure building package control procedures and property removal permits are strictly enforced.
8. In high-risk environments:
    - Establish entry control procedures or install access control equipment commensurate with the sensitivity or value of the resources involved.
    - Install an intrusion detection system that acts as a deterrence to intrusion and alerts security personnel of an actual intrusion.