Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 0730/4
Transmittal Sheet
March 29, 2013

SECURITY AND LAW ENFORCEMENT

1. **REASON FOR ISSUE:** This Handbook establishes mandatory procedures for protecting lives and property within VA's jurisidiction, by updating Appendix B, "Physical Security Requirements and Options." This issue provides updated requirements for securing temporary storage facilities of information technology equipment, and providing other updated physical security requirements.

2. **SUMMARY OF CONTENTS AND MAJOR CHANGES:**

a. **Summary.** This replaces Appendix B of VA Handbook 0730, August 11, 2000. This Appendix sets forth specific requirements and options for protecting VA people and assets.

b. **Major Changes**

(1) Inserted physical security requirements specific to protecting VA information technology assets in temporary storage or staging areas.

(2) Inserted a policy requirement for annual physical security surveys of key activities and spaces withinVA's jurisdiction.

(3) Corrected errata and misnumbered paragraph items in the previous version of this Handbook.

3. **RELATED DIRECTIVES:** VA Directive 0730, *May 27, 2010.*

4. **RESPONSIBLE OFFICE:** The Police Service (07B), Office of Security and Law Enforcement, Office of Operations, Security, and Preparedness is responsible for the material contained in this handbook.

5. **RESCISSION:** Appendix B of VA Handbook 0730/2 *May 27, 2010* is rescinded and replaced with this version.

CERTIFIED BY:

/s/
Stephen W. Warren
Acting Assistant Secretary
for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Jose D. Riojas
Assistant Secretary
Operations, Security, and Preparedness

PHYSICAL SECURITY REQUIREMENTS AND OPTIONS

(X) - Applicable Requirements, (O) - Optional Measures

Location	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Canteen Retail Store	X	O	X	X	X					X	X					X	X	X	
Canteen Storage Area	X	O	X	X	X					X	X				X	X	X	O	
Canteen Office	X	O	X	X	X		X			O	X				X	X	X	X	
Agent Cashier	X		X	X	X		X			O	X				X		X	X	
Pharmacy Drug Storage Room	X	X	X	X	X			X	X	O	X		X				X	O	
Pharmacy Dispensing Area	X		X	X	X	X				O							O	X	
Pharmacy Manufacturing Area	X		X	X	X				X	O	X						X	X	
Veteran Records-Long Term Storage	O	X	X	X	X						X						O		
Warehouse Storage/ Bulk	O	X	X	X	X						X					O	X	O	
Primary Inventory (Medical Supplies)	O	X	O	O	O					O	X					O	O	O	
Laundry Plant	O		X	O	O						X						X		
Central Linen Issue	O		X	X	X						X						X		
New Linen Storage	X		X	X	X						X						X		
IT Data Centers and Server Rooms	X		X	X	X					O	X						X	X	
Telephone Equipment Room	X		X	X	X					O	X						X		
Animal Research Facility	X		X	X	X				O	O	X					O	O	O	X
Ward and Treatment Rooms												X	X	X		O	O	O	
Medical Media Equipment Rooms	X	X	X	X	X					O	X				X		X		
Evidence Storage	O	O	X	X	O					O	X				O	O	X		
Weapon Storage/Armory	X	X	X	X	X					O	X				O	O	X		
Research/Clinical Labs[1]	O	O	O	O	O						X	X	X				X	O	
Radiation-High-risk[2]	O		O	O	O					O	X						X		
Radiation-Low-risk[3]	O		O	O							X						X		
Commercial Electrical Power Connections[4]	X	O	X	X	O					O	X								X
Commercial Telecommunication and Data Connections[4]	X	X	X	X	X					O	X						X		O
Compressed Medical Gas Bulk Storage (including LOX or propane)[4]	X	X	X	X						O	X						O		X
Child Care Facilities	X		X		X					X					X		X	O	X
Electronic Fingerprint Capture/PIV ID Production Equipment			X	X							X						X		
Informal IT Temporary Storage/staging areas			X	X							X						O		
IT Telecomm/Data Connection Closets		X	X	X							X						O		
IT Equipment Storage Rooms (permanent)	X	X	X	X						O	X						X		
Legal Hearing and Client Consultation Rooms																		X	

[1]Where substances on the CDC or VA watch list are stored, maintained or produced

[2]Location or room where the total activity of a single radionuclide with a half-life of more than three days or is more than one Curie is received or stored.
[3]Any location other than defined as "radiation high-risk" where radioactive materials and/or radiation sources are received, stored or used.

[4]Where located outside of buildings, will have a seven foot tall (minimum) fence and be well lit during hours of darkness.

1. Requirements and Optional Measures Defined. The following are minimum acceptable standards. These standards may be exceeded if indicated by a risk assessment. Facilities should consult with the OS&LE when planning major security upgrades. Requests for waivers from these standards may be addressed to the Infrastructure and Policy Division of OS&LE (07B1C). Such requests will include:

a. Facility or other VA activity identification
b. Full description of the project, with a VA point of contact
c. Specific standard for which the waiver is requested
d. Suggested alternative mitigation for the project
e. Please note any Federal or other standard that addresses the alternative mitigation.
f. Expected benefit of the alternative mitigation, including cost savings (if any). An assessment of whether the alternative mitigation will meet the Department's requirement to protect people, property and assets.
g. OS&LE will review the request and return a response within 14 calendar days of receipt.

A - Windows. When below 12 m (40 ft.) from ground level or the roof of a lower abutment, or less than 7.5 m (25 ft.) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, security mesh screening for windows is required. Security measures that exceed these requirements may be authorized in writing by OS&LE. Required specifications for stainless steel security mesh screening are:

1. All #304 stainless steel woven mesh 0.7 mm (.028 in.) wire diameter, with tensile strength of 15 kg/mm (800 pounds per linear inch).

2. Mesh 12x12 per 25 mm (1 in.) with main and sub frames of 2.7 mm (12 gauges) carbon steel with baked enamel finish and internal key locking slide bolts.

B - Walls. Exterior walls of brick and masonry construction are acceptable. Exterior walls which are composed of wood frame and siding require an interior backing of steel security screen mesh or sheet partition. Pharmacy and Agent Cashiers perimeter walls shall be full height, floor to underside of slab above. Interior walls containing dispensing windows shall be a minimum of 100 mm (4 in.) solid concrete masonry units to ceiling

height with either masonry or gypsum wallboard to underside of slab above. Bulk control substance storage vaults require perimeter walls of brick or masonry construction full height.

C - Doors and Door Locks. The locking requirements (including access-controlled egress doors) outlined in National Fire Protection Association (NFPA) Life Safety Code standard, latest edition, 101-7.2.1.5 and 7.2.1.6 must be followed.

1. Door Construction: Doors are of 45 mm (1-3/4 in.) solid core hardwood or hollow steel construction. Dutch or half doors are unacceptable. Removable hinge pins on door exteriors must be retained with set pins or spot welded, preventing their removal. This applies only if the hinge pins are on the outside of the doors and door frames. Hinge pins will be on the outside if the door opens outward.

2. Mechanical locking systems. Where mechanical lock systems are used, installed lock sets must allow for single motion egress. The installation of high security exit devices meeting NFPA Life Safety Code standards is appropriate.

(a) Glass doors or doors with glass panes must have one lock set that is key operated from the interior of the protected area.

Note: Fire code prohibits locks from being locked from the inside that require a key to exit. The intent is that there must be two locks, one of which must be key operated. The other lock can be key, combination or electronic. (NFPA 101, 7.2.1.5.2 Locks if provided, shall not require the use of a key, a tool or special knowledge or effort for the operations from the egress side

(b) Steel doors will not be set into wooden frames.

(c) Doors set in steel frames must be fitted with a mortise lock with a deadlock feature. IAW ANSI/BHMA A156.13 American National Standards for Mortise Locks

(d) The day lock on the main door must be automatically locking, with a minimum 19 mm (3/4 in.) dead bolt and inside thumb latch. Combinations or keys to day locks will be restricted to service employees and combinations changed immediately on the termination or reassignment of an employee. See paragraph 8 of this appendix for a detailed description of key control systems.

3. Electronic/Magnetic locking systems. Where installed, electronic locking systems will include an automatic “request to exit” sensor and a “push to exit” manual lock release switch. Refer to the NFPA Life Safety Code for details.

D - Other Room Access Means. Interstitial overhead areas which enable entry into a secure room from an unsecured room must be barricaded by the installation of a suitable partition in the interstitial space which prevents "up and over" access. Openings

in construction above ceilings or below raised access floors shall be protected as below requirement.

All vents, ducts, and similar openings in excess of 96 square inches (620 cm2) that enter or pass through space shall be protected with either bars or grills. If one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm2), bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six (6) inches (150 mm) on center; if grills are used, they must be of 9-gauge expanded steel.

E - Motion Intrusion Detectors. An intrusion detection alarm system which detects entry into the room and which broadcasts a local alarm of sufficient volume to cause an illegal entrant to abandon a burglary attempt. Intrusion detector equipment which operates on the principle of narrow beam interception, door contacts, microwave, or photoelectric eyes are unacceptable as the primary means of detection. Intrusion detectors must have the following essential features.

1. An internal, automatic charging DC standby power supply and a primary AC power operations.

2. A remote, key operated activation/deactivation switch installed outside the room and adjacent to the room entrance door frame and/or a central alarm ON-OFF control in the Police office or other monitoring location.

3. An automatic reset capability following intrusion detection.

4. A local alarm level of 80 dB (min) to 90 dB (max) within the configuration of the protected area.

5. An integral capability for the attachment of wiring for remote alarm and intrusion indicator equipment (visual or audio).

6. A low nuisance alarm rate as defined in VA Master Specifications, Division 28 - Electronic Safety and Security "28 16 11 INTRUSION DETECTION SYSTEM."

7. Installation Notes

(a) A locally sounding alarm should not be installed in a room which is close to an ICU, cardiac care, or other special treatment areas where a loud alarm would have an injurious effect on patients.

(b) In addition to the locally sounding alarm, remote visual and/or audio annunciators must be at a location within the facility which ensures 24 hour monitoring. These annunciators will have the capability of identifying individually protected zones.

(c) In protected rooms of outpatient clinics not on facility grounds, intrusion detector alarms may be routed to a commercial security alarm monitoring firm, a local police department, or a security office charged with building security. The remote alarms will be in addition to locally broadcast alarms in the protected areas.

(d) Remote bulk storage warehouse facilities will have one or more local broadcasting alarms inside and outside of the protected area.

(e) When replacing existing systems, or purchasing new, consideration will be given to intrusion detection equipment that integrates with CCTV and physical access control systems.

F - Pharmacy Dispensing Counter. Windows and walls of pharmacy dispensing must meet the U.L. Standard 752 for Class III Ballistic Level. VA Architectural Standard Detail 67 B applies to pharmacy dispensing windows but the window should be set in a minimum 100 mm (4 in.) solid concrete masonry units to ceiling height with either masonry or gypsum wallboard to underside of slab above.

G - Agent Cashier Counter. Bullet resistive service windows must meet the U.L. Standard 752 for Class III Ballistic Level. VA Architectural Standard Detail 67 applies to cashier counter construction. Applicable also to other cash transaction facilities. The windows should be set in a minimum 100 mm (4 in.) solid concrete units to ceiling height with either masonry or gypsum wallboard to underside of slab above

H - Bulk Drug Storage Safes and Vaults. Drugs classified as schedule I, II, or III (narcotic controlled substances under the Controlled Substance Act of 1970 must be stored in safes or vaults which conform to the following specifications:

1. Safes will be GSA class 5 security containers weighing no less than 340 kg (750 pounds).

2. Where bulk quantities or controlled substance handling requirements deem safes impractical, vaults must be used. Specifications for two types of vaults are given: Type I for outpatient clinic or center use, and type II for construction in medical centers only. The type I vault is not as formidable and permanent a structure as the type II concrete vault and, therefore, schedule I, II, and III (narcotic) controlled substances may not be stored on open shelving within the type I vault. To compensate for the lower security of type I vaults lockable steel cabinets installed within the vault must be used for schedule I, II, and III (narcotic) substances. Vault specifications are as follows:

(a) Type I Vault. Enclosure constructed of steel security screen, woven mesh, 1.2 mm (.047 in.) wire diameter alloy #304 stainless steel, with tensile strength of 29 kg/mm (1,600 pounds per linear inch). Mesh 10 x 10 per 25 mm (1 inch) with main frame and sub frames of 2.4 mm (13 gauge) alloy #304 steel. In rooms with dropped ceilings, the vertical frames and mesh walls must meet the actual ceiling or a security mesh ceiling

installed below the false ceiling. In lieu of security mesh screening enclosures, type I vaults may be constructed of 2.4 mm (13 gauge) steel wall partition material with corner brackets welded and floor/ceiling anchors firmly set to prevent disassembly. Mesh vaults may be enclosed with drywall or paneling with appropriate ventilation openings.

(b) Type II Vault. Constructed of walls, floors, and ceilings of minimum of 200 mm (8 in.) reinforced concrete or other substantial masonry, reinforced vertically and horizontally with 13 mm (1/2 in.) steel rods tied 150 mm (6 in.) on center. Doors and day gates must meet GSA class 5 criteria. Vault ventilation and utility ports may not exceed 0.06 m^2 (100 square in.) in area.

I - Bulk Drug Storage Cabinets. Steel cabinets with adjustable shelving and built in locking devices are required for the storage of bulk supplies of schedule III, Non-Narcotic, to V controlled substances.

J - Closed Circuit TV. Security Surveillance TV camera with motion detector feature on cameras and at monitor location. Telecommunications Support Service (197) may be contacted for obtaining technical assistance. See VA Handbook 0730, Part E for further details and considerations.

K - Special Key Control. Room door lock keys and day lock combinations, where applicable, are Special Keys as defined in paragraph 9.d.(10) of this appendix.

L - Drug Cabinets. Key locked, all steel cabinets, firmly anchored in place are required for ward, emergency room or treatment room storage of small quantities of controlled substances. Locked unit dose carts are acceptable; but must be positioned in a supervised area when not in use. Glass front drug cabinets are not acceptable for controlled substance storage. Plexiglas front cabinets 10 mm (3/8 in.) or greater in thickness, are acceptable.

M - Refrigerators. To be equipped with a built in lock mechanism or hasp with padlock when used to store controlled substances (all schedules) and other potentially dangerous drugs and when located outside a locked or attended drug storage room.

N - Medical Supply Rooms and Closets. Service key control and accountability are required in accordance with paragraph 9.(d)10.

O - Cash Safes, Cabinets, and Lockers. For the security of cash deposits and valuables, safes, cabinets, or lockers meeting the following criteria should be used. The size and configuration of commercially available safes, cabinets, and lockers are optional.

1. The minimum requirement for the storage of currency or negotiable instruments is a container that is resistant to 20 man-hours surreptitious entry, 30 man-minutes covert entry and 10 man-minutes forced entry or greater. Commercial burglary resistant safes

meeting this requirement and approved for use are certified by Underwriters' Laboratories, according to the following classifications:

a. Tool-Resistant Safe - TL-30
b. Torch and Tool-Resistant Safe - TRTL-30
c. Torch and Tool-Resistant Safe - TRTL-60
d. Torch, Tool & Explosive Resistant Safe – TXTL-60

2. Safes rated as Tool-Resistant Safe- TL-15 are not acceptable.

P - Secure Property Storage Containers. For bulk retail merchandise, medical supplies and other items requiring off-shelf protection, steel storage cabinets with adjustable shelving are available through the Federal supply service, group 71, class 7125.

Q – Electronic Physical Access Control Systems (PACS). For monitoring and controlling access to areas identified as requiring high or medium levels of assurance. PACS systems are not used for recording employee time and attendance.

1. Access Safeguard. To prevent learning codes through keypad observations or use of stolen or found access cards.

2. Time Sensitive. The ability to program access by user, by shift and day.

3. Area Sensitive. The ability to program access by door and area for each individual user.

4. Fail-Safe. The ability to maintain access security if the system goes down (i.e. bypass key).

5. Access Record/Audit Trail. The ability to provide for periodic or on demand print-out of names and time/dates of individual accessing. Records of access or audit trails will not be used for employee time and attendance purposes.

6. User Coverage. The number of individual access codes that the system will accommodate.

7. Personal Identifier Number (PIN) Codes. Access control systems protecting PACS high security areas, such as controlled substance storage, primary computer and communications rooms, research or clinical laboratories that store, use or develop biohazardous materials, require a PIN number as a secondary personal authentication to be used in addition to card readers. "Scramble Pad" type PIN readers are recommended when PIN systems are installed. See the table below for specific VA-identified required locations.

8. Biometric Systems. Biometric security systems are those that use a personal measurement, such as fingerprints, hand geometry, facial geometry or iris scans, as authentication. Biometric devices can be used in lieu of PIN systems in PACS high protected spaces, but only as a secondary form of authentication. Biometric measurements may also be used in addition to a PIN in high security applications.

9. Compliance with Federal Standards. New installations or retrofitted access control systems will be compliant with technology described in Federal Information Processing Standard (FIPS) Publication 201, Personal Identity Verification of Federal Employees and Contractors, and the document "PACS Implementation Guidance, Version 2.2 (July 30, 2004), published by the Physical Access Interagency Interoperability Working Group of the GSA Government Smart Card Interagency Advisory Board. This requires that such systems will meet the ISO/IEC 14443 a, Parts 1-4 standard for contactless (proximity) card systems, or the ISO/IEC 7816 Standard for contact-type cards. Facilities may continue to use existing PACS that operate on older technology (Magnetic Stripe, 2nd Generation bar code, etc.) as an interim measure until replacement systems are acquired and installed as part of normal equipment lifecycles. Further information on VA Smart Card operated PACS requirements can be found in the most recent edition of the document: "Physical Access Control Recommendations for the Department of Veterans Affairs." Guidance and assistance with the standards can be obtained from the OS&LE.

10. PACS Assurance Level Designations

(a) PACS provide a level of assurance regarding the identity of persons entering a protected space. The levels of assurance required are determined as a result of vulnerability or risk assessments and physical security surveys. In addition, the following chart indicates minimum requirements for specified VA protected activities. For purposes of this policy, levels of assurance are defined as:

High - Entry requires a valid access card used in conjunction with a secondary form of authentication. Either a Personal Identification Number (PIN) known only to the card holder, or a biometric measurement, or both, is used as the secondary authenticator.

Medium - Entry requires the use of a valid access card.

Low - Entry requires the visual authentication of a valid access card or facility identification card. The card may be inspected by a police officer or other designated staff upon entry into the protected space, or may just require that it is worn at all times in a visible manner; see VA Directive 0730, paragraph 2.n.

Facilities may choose to use a more stringent protection level for any of these locations. In addition, facilities may choose to protect other activities with PACS.

The following are minimum protection and assurance levels for facilities that have installed PACS:

Location	PACS Assurance Level
Canteen Retail Store	Medium (during hours of closure)
Canteen Storage Area	Medium
Canteen Office	High
Agent Cashier	High
Pharmacy Drug Storage Room	High
Pharmacy Dispensing Area	Low
Pharmacy Manufacturing Area	Medium/(High for Controlled Substances)
Veterans Records-Long Term Storage	Medium
Warehouse Storage/Bulk	Medium
Primary Inventory (Medical Supplies)	Medium
Laundry Plant	Medium
Central Linen Issue	Medium
New Linen Storage	High
IT Data Centers and Server Room	High
Telephone Equipment Room	High
Animal Research Facility	High
Ward and Treatment Rooms	Low
Medical Media Equipment rooms	Medium
Evidence Storage	High
Weapon Storage/Armory	High
Research/Clinical Labs	Medium/High (see footnotes on page B1)
Radiation-High Risk	High
Radiation-Low Risk	Medium
Commercial Electrical Power Connections	High
Commercial Telecomm/Data Connections	High
Child Care Facilities	High
Electronic Fingerprint Capture Systems	Medium
IT Equipment Storage Rooms (permanent)	High
Informal OIT Storage/Temporary Storage/Staging Areas	Medium
IT Telecomm/Data Connection Closets	High

R - Robbery/Panic/Duress Alarms. These types of alarm systems are used to provide rapid notification of police during an actual incident. The alarm may be activated by a covertly placed switch or button. Once activated, the switch or button can only be re-set by a key or other special tool that is in the possession of the VA police unit or other responder. The alarm annunciator will be monitored by police whenever the protected area is operational. The exact location of panic/duress alarm switches will be determined by a physical security survey of the protected area.

Panic/Duress alarms will always be installed in the interior of pharmacy controlled substance or other Type I or Type II vaults.

S - Perimeter Barriers. Perimeter barriers are defined as concrete bollards; concrete filled steel bollards; or concrete planters. Appropriate fencing may also be a perimeter barrier, depending on the application. Barriers must be of sufficient strength/weight to stop a passenger-car sized vehicle from breaching the protected space. For Child Care Centers, a minimum 7 foot height vinyl coated 6 gauge core steel fence will be erected around all playground areas and around areas containing multiple non-primary entrance doors.

2. Special Security Requirements: Biohazardous or Radioactive Materials in Research or Clinical Laboratories.

a. Police Chiefs will conduct vulnerability assessments of any clinical or research laboratory under VA Police jurisdiction. Records of the assessments will be maintained in Police administrative files (RCS-10) This includes any such laboratory in VA owned or leased space that is not located on or contiguous to the main facility campus. This also includes laboratory facilities physically located on VA owned or operated property, but that are leased to outside entities, such as universities, non-profit organizations and others.

(1) Initial assessments will be focused on determining whether materials are present that have been identified by the Centers for Disease Control and Prevention (CDC) or VA as potential biohazards. Descriptions of these materials are found at Title 42 Code of Federal Regulations (CFR), Part 73. An updated listing of select biological and chemical hazardous agents is maintained by the CDC and is located at: http://www.bt.cdc.gov/agent/agentlist.asp.

(2) As part of the assessment, Chiefs of Police will carefully review memoranda of understanding, contracts or other agreements related to the use of Department properties by non-VA entities. The document review is focused on assuring the careful delineation of security responsibilities for the laboratory space. The intent is to ensure that VA security policies, practices, and procedures are applied and followed.

b. If the initial assessment finds that such materials, or radioactive materials, are, or may be, present in VA laboratories, the assessment will then be focused on determining vulnerabilities in physical security and recommended corrective actions. Corrective actions will be consistent with the physical security matrix in this appendix, but more stringent measures may be adopted where necessary. In addition, the laboratory will be added to the facility annual physical security survey program, and surveyed once every 12 months.

c. When the listed materials are found, or isolated from a patient, and appear to be evidence of potential criminal activity, e.g., anthrax threats, etc., the local VA Police unit

will be contacted and an evidentiary chain of custody established. The investigating VA Police officer will initiate appropriate reporting and notification actions.

d. The facility Director will ensure that security training, appropriate to facility security systems, is provided for all employees, without compensation employees, and volunteers working in clinical or research laboratories.

3. Special Security Requirements: Electronic Fingerprint Capture Systems.

a. Electronic fingerprint capture equipment is used to digitally obtain fingerprint images. Typically, these systems are used to transmit fingerprints to other Federal agencies for either employee background or criminal investigation purposes.

b. Generally, fingerprint capture systems consist of a laptop or desktop computer that has a secure data connection to the Internet. Fingerprint collection platens and other equipment is connected to the computer.

c. All of the components of the fingerprint system will be stored in locked rooms or cabinets when not in use. Locks will be Special Keyed (see paragraph 9.d.(10)) or protected by a PACS under the Medium level. Access will be strictly limited to authorized system operators.

4. Special Security Requirements: Storage and Control of Radioactive Materials.

a. The VA Police Chief must coordinate with the Radiation Safety Officer and Radiation Safety Committee to implement procedures to preclude unauthorized removal or access to stored radioactive materials.

b. The VA Police Chief must coordinate with the Radiation Safety Officer and Radiation Safety Committee to implement procedures to control and maintain continuous surveillance of radioactive materials that are not in storage.

5. Special Security Requirements: Bulk Storage Media/Informal OIT Storage/Temporary Storage/Staging Areas.

a. All physical input and output products of VA systems that contain privacy protected data, to include papers, disks, computer drives, and other mediums of storage that contain information, must be protected against misuse and unauthorized access, disclosure, modification, or destruction and stored in a controlled area.

b. The requirements established in this section of Appendix B are in addition to, and do not change, those found in VA Handbook 7002 "Logistic Management Procedures" (July 10, 2009). Paragraph 11 of that Handbook addresses IT Inventory Storage.

c. Informal OIT Storage/Temporary Storage or Staging areas are defined as locations used for the temporary staging of OIT equipment during the process of installation or

deployment. This is defined as "temporary" or "informal" because the room or area being used for this purpose may not have permanent technical aids to security installed, or otherwise not originally intended for equipment storage. The VA facility will take steps to establish the informal or temporary storage location as a controlled area.

d. OIT will notify the servicing VA Police or other security organization when such storage is being planned. On VHA facilities, the VA Police will conduct an initial assessment of the temporary space, and will continue to monitor the physical security of that space. The informal or temporary storage space will be added to the facility's annual physical security survey program. Records of those physical security surveys are maintained in VA Police files at a VHA facility or collocated (VHA/VBA/NCA) campus. In VBA or NCA locations that are not serviced by a VA Police unit, the facility director will maintain the survey records and actions taken. When there is no longer a need for the controlled area, the facility will discontinue annual physical security surveys of that location. In addition to discontinuing annual physical security surveys, special keying will be discontinued and the space lock keyed to the facility master key system.

e. A controlled area is generally defined as an area or space that has a minimum of single-barrier protection. Physical security requirements C, D, and K from above are recommended. Requirement Q, PACS, should be considered. The establishment of controlled areas and their physical security requirements is a risk based decision.

f. Informal OIT Storage/Temporary Storage/Staging Areas will be special keyed as described in paragraph 9.d.(10) below, and access strictly limited. The OIT program manager with responsibility for the controlled area will determine the need for access.

6. Special Security Requirements: Domiciliary and Long-Term Care

a. Dorniciliary, Nursing Home Care units and other long-term residential care facilities are subject to existing VA physical security standards for the storage of DEA Schedule II through V drugs. Such units will be surveyed annually as part of the facility physical security survey program. The physical security requirements for Pharmacy Drug Dispensing Area, as outlined in this Appendix will be followed.

b. The VA Chief of Police will consult regularly with the Chiefs of these units, and with the facility official responsible for narcotic inventories.

c. The Office of Security and Law Enforcement will review records of these surveys during routine program inspections.

7. Mail Rooms.

a. For the purposes of this policy, Mail rooms are defined as rooms, buildings or other enclosed locations within a facility or campus that are used solely for receiving, sorting and distribution of mail and small packages.

b. Potential threats to VA mailrooms can include mailed explosive devices, chemical or biological agents. Theft of mailed materiel is also a potential threat.

c. Mail rooms should be located away from other high risk activities, and, to the extent possible, on independent air handling or ventilation systems. Mail rooms are an appropriate location for package and mail screening equipment.

d. Mail rooms will be special keyed, as defined in paragraph 9.d. (10) of this Appendix. Consistent with local facility vulnerability assessments, mail rooms may also be protected with PACS.

8. Physical Security Surveys

a. Physical security surveys and appropriate follow-up surveys are conducted of the locations identified in the Page B-1 matrix of this Appendix. Surveys will be conducted at a minimum of once every twelve months. Surveys will be conducted in accordance with the training provided in VA Police Training Unit #11, Physical Security.

b. When these protected assets and controlled areas are located in VA properties that are not contiguous to a VA medical center or campus (Community Based Outpatient Clinics, for example) they are still subject to the physical security surveys defined in Paragraph 8.a.

c. Results of each survey will be routed through the VA facility director to the service chief with responsibility for the protected space. An action plan for mitigation of security risks will be sent by the responsible service chief to the VA chief of police. Records of surveys and mitigation plans will be maintained in VA Police RCS files.

d. Facilities that do not have a matrix- identified activity, such as Child Care Centers, are not required to conduct or keep a record of such surveys.

e. Records of facility physical security surveys are reviewed as part of routine police program inspections conducted by the Office of Security and Law Enforcement.

9. Space Key Control.

a. The development, refinement and maintenance of a lock key production, issuance, inventory, accountability, and rapid key change system is a responsibility of each facility. Traditionally, this responsibility has been placed under the Engineering Service, but it may be more appropriate at some facilities to place the key control function within the VA Police unit. The facility Director will determine the appropriate organizational location of the lock shop.

b. In buildings operated by the Administrator of General Services, space lock key service is provided by the GSA Building Manager. However, special lock and key controls for high risk areas (pharmacies, clinical and research laboratories, server and

telecommunications rooms etc.) will be determined by the facility Director or designee, who will establish and maintain a key control system for these spaces.

c. Objectives of Space Key Control Systems

(1) Maximum zone security with a minimum of room and area door locks;

(2) A centralized and rigid control of key production;

(3) Decentralized responsibility for keys in use within service zones to respective service chiefs;

(4) A recorded chain of accountability for each room and area key to key users, directly to or through the user's service chiefs;

(5) The elimination of hybrid key lock hardware and key inventory systems; and

(6) Attaining the capability for rapid room and area lock and key changes for restoring security following the loss or theft of keys..

d. Key Control Systems Definitions.

(1) Space - denotes fixed and permanent property with areas and rooms having doors or passive barriers, as distinguished from storage compartments or other movable containers.

(2) Room - a permanent structural compartment, defined by walls and doors.

(3) Area - two or more contiguous rooms distinguishable from other spaces by common functional activities.

(4) Zone - space containing rooms and/or areas designated for the primary use of a particular service or element to carry out its functional activities. Establishment of keying or alarm zones should be one result of physical security surveys conducted as described in VA Handbook 0730, Part E.

(5) Common Space - Rooms or areas contiguous to service zones, but neither included in a service zone nor exclusively controlled by a particular service or other chief.

(6) Great Grand Master Key - A key which is capable of operating most or all lock devices within a key system, except for locks operable by special keys.

(7) Grand Master Key - One which is capable of operating only a segment of all locks within a key system.

(8) Master Key - A key that is capable of operating only a portion of that segment of locks in a system that may be opened by a grand master key.

(9) Individual Key - A key which can only operate one lock.

(10) Special Key - A key which can only open a lock in a high risk or sensitive area (locally determined), and which cannot be opened by a great grand master, grand master, master or any other individual key. Special keys may also include those that can only open certain doors for cleaning, maintenance, construction, mental health units, etc.

e. Key Issuance Procedures.

(1) All facilities will use a 4 control level keying system as described:

(a) Great grand master key level operating all space doors except those to special key areas;
(b) Grand master key level for each service zone;

(c) Master key level for use with service zones as needed. Use of this level will be minimized; and

(d) Individual key level. The special key is not considered to be a distinct keying level.

(2) Outpatient and other facilities that are not located on VAMC campuses will use a 2 control level system of master, individual and special keys.

(3) Great grand master keys will operate all space door locks of a facility except for those indicated in the security matrix in this appendix as requiring special keys. In addition, other areas that require this special protection may be identified by facility managers and specially keyed locks may be installed. Examples of other special key locations are, but are not limited to residential quarters, post office facilities, police operations room, etc. A duplicate special key to each of these areas will be kept in separate sealed envelopes in a locked cabinet in the VA Police unit. Envelopes will be sealed in a manner which precludes being opened without detection. Use of these keys is limited to emergencies, and will be authorized by the appropriate official such as a service chief or previously designated official responsible for the specially locked area. Any use of special keys, as defined in this paragraph, will be recorded in the VA Form 1433, VA Police Daily Operations Journal. On the next business day following an emergency use of a duplicate special key, the employee who requested the emergency use will provide a written report to the official in charge of the protected area, setting forth the circumstances that led to the key use.

(4) The number of great grand master keys at a facility will not exceed five and these will receive special protection in recognition of their potential for neutralizing the entire locking system of a facility if stolen or reproduced without authorization. Great grand

master keys will be authorized for issuance, with the limit of 5, on an actual need basis. Normally, a facility Director, Associate or Assistant Director and Chief of Staff should possess great grand master keys. The Chief Engineer or equivalent facility manager and the Chief of VA Police will also be issued a great grand master key each. The key assigned to VA Police will be available to the on-duty police supervisor on a 24 hour daily basis. The use of this key by a VA Police Supervisor will be recorded in the VA Form 1433. Procedures will be established for the temporary use of the great grand master key under the control of the Chief Engineer or equivalent facility manager by other service chiefs on those occasions when unlimited space access is required.

(5) It is the responsibility of service chiefs to determine keying needs for their zones of responsibilities, originate all key requests, receipt for keys issued, and maintain intra-service key issue receipt records. Each service chief will be issued no more than three grand master keys (service grand masters) which operate all room and area door locks in his/her zone or control. Master keying within a service zone and the designation of rooms within each zone for which individual keys are required will be outlined by each service chief in a service zone keying plan. In developing service zone key requirements, the service chief will consider which secured space will require after hours access by housekeeping personnel and to group these spaces under a single master key for issue to Housekeeping or Facilities Management, as appropriate.

(6) Quantitative requirements for service master and individual keys will be kept to a minimum with particular attention given to minimizing requirements for individual keys to rooms located within areas that are secured or attended 24 hours daily. Facility and service clearance procedures will include the requirement that Department employees return issued keys to the issuing service prior to clearance approval.

(7) The manager of the key production operation who may be either the Chief Engineering or facility equivalent or Chief of Police, as appropriate, will accept only those requests for key reproduction which have been approved by the service chief having zone responsibility. The Request and Engineering Work Order, VA Form 3213b, is prescribed for key issue or lock change requests. Service requested keys will be delivered either to the service chief originating the request or to a designated service key control representative.

(8) The facility is responsible for the establishing a keying plan for rooms, areas and zones falling into the category of common space. Building common space hardware may be grand master keyed, or master keyed by floor level or function. However, lock hardware on building entrance doors will not be master keyed with any service zone or common space master(s) within the building. Building entrance doors should be keyed to the great grand master key only; however, these doors can be keyed for an individual key on an actual need basis. These common space keying plans will be used by the facility to maintain space key control and overall accountability.

f. Basic Lock Hardware Specifications

(1) All space lock hardware will meet the appropriate requirements outlined in the security matrix of this appendix.

(2) Space door locks will have interchangeable cores that can be removed from the locking mechanism only by the use of a special control key or tool. The control key or tool will fit all interchangeable core hardware, including those operated by special keys. All cores are to be so constructed that they will be instantly interchangeable into the core housings of all mortise locks, rim locks, cylindrical locks, and any other type of lock included in the great grand master key system.

(3) All cores will be of 6 or 7 pin construction, depending on facility size and projected combination code requirements, and will be constructed so that the mortise cylinder cam or rim cylinder spindle is not directly attached to the core. Spindles and cams will be a part of the construction of the cylinders so that cores need not be altered in any way when they are interchanged from one type of lock to another. All cores will therefore be instantly and completely interchangeable.

g. Basic Key Production and Control System Requirements

(1) Key Production

(a) A commercially provided combinating code pattern listing. (Note: "combinating" is a technical locksmithing term relating to the pattern of pins within a lock core.)

(b) A key making machine for the cutting of keys by code rather than from pattern keys.

(c) A hand combinating kit with precision pins so that cores may be recombinated with the necessity of filing pins to fit shear lines.

(d) A set of letter and number dies for core and key marking and needed core installation tools.

(2) A file system for accountability, reproduction and change of issued keys. May either be a cross index file card (hardcopy) or electronically automated system, which records, at minimum, the following information:

(a) Lock cores to doors by room or area door numbers.

(b) Room or area door numbers by lock core numbers.

(c) Service chiefs or individuals holding keys in an alphabetical employee file which lists all keys issued to each person by key number.

(3) To ensure the integrity of the lock key system, the following steps will be taken:

(a) Pattern keys will not be used, and turned-in keys will be destroyed rather than maintained. Duplicates of issued keys, except special keys in secured and sealed envelopes, will not be maintained.

(b) Keys produced will not bear identifying markings, such as "VA" and/or "US Government."

(c) The loss or theft of VA space keys will be reported as soon as noticed to the servicing VA Police unit. If the VA police investigation does not immediately result in the recovery of the key, or a positive determination is made that the loss occurred off of facility property, the key cores operable by the lost key will be changed and all affected keys replaced within five days.

(d) Persons found to be in unauthorized possession of VA keys, or in possession of unauthorized reproductions of such keys, will be cited by VA Police for the appropriate violation of Title 38 CFR 1.218.

(e) The interchangeable core system control key, key cutting machine, all lock service and combinating kits, and combinating records will be secured in a locked cabinet or room. This is an appropriate application for a special key. The functions of lock core combinating, key production and record maintenance will be performed by a qualified locksmith, or a maintenance employee qualified by the lock system manufacturer in their products.

(f) Key issuance and control procedures are:

(1) General

Guidance on procedures for keys, locks, and locking devices. Directors will establish procedures for the protection of locks, keys, and combinations used to secure facilities, vaults, and containers in which controlled medical substances and VA sensitive items are stored. The number of people with access to keys and combinations will be the minimum necessary for efficient operations.

(2) Key custodian and alternate custodian
A primary or alternate key custodian is the person who will—

(a). Be appointed, in writing, to issue and receive keys and maintain accountability for facility keys and locks.

(b). Ensure that individuals designated to issue, receive, and account for keys and locks in his or her absence, clearly understand local key control procedures.

(c). Maintain a key control register at all times to ensure continuous accountability for keys.

(d). Be listed on an access roster.

(3) Access roster
The names and duty positions of personnel authorized unaccompanied access to the key depository will be posted on or in the vicinity of the key depository. Access roster will be signed by the appointing authority.

(4) Key control register
Keys will be signed out to only authorized personnel, as needed, on a key control register. The key control register (Key Control Register and Inventory) will be used for the purpose. When not in use, the key control register will be kept in a locked container with controlled access.

(5) Key depository

(a). A lockable container, such as a safe or filing cabinet, or a key depository made of at least 26–gauge steel, equipped with a tumbler–type locking device and permanently affixed to a wall, will be used to secure keys.

(b). The key depository will be located in a room where it is kept under 24–hour surveillance or in a room that is locked when unoccupied.

(6) Key and lock accountability
(a). Keys and combinations to locks will be accounted for at all times. Keys to locks in use which protect the property of the facility will be checked at the end of each duty day. Differences between keys on hand and the key control register will be reconciled.

(b). Keys will be inventoried by serial number semiannually. A written record of the inventory will be retained until the next inventory is conducted.

(c). When a key is lost or missing, an inquiry will be conducted. The lock will be replaced or re-cored at the decision of the Director.

(d). A key and lock inventory will be maintained which includes a list of all of the following:
(1) *Keys.*
(2) *Locks.*
(3) *Key serial numbers.*
(4) *Lock serial numbers.*
(5) *Location of locks.*
(6) *The number of keys maintained for each lock.* This list will be secured in the key depository.

(e). Keys and locks which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

(7) Combinations to locks will be recorded sealed in the envelope and stored in a locked container with controlled access. A signature or seal will be placed over the envelope flap to identify tampering.

KEY ISSUE AND TURN IN (*Continues*)

KEY NUMBER	ISSUED (Date/Time)	ISSUED BY (Printed Name/Signature)	ISSUED TO (Printed Name/Signature	TURNED IN (Date/Time)	RECEIVED BY (Printed Name/Signature

INVENTORIES

DATE	PRINTED NAME/SIGNATURE	DATE	PRINTED NAME/SIGNATURE