Military Police

FORT KNOX PHYSICAL SECURITY PROGRAM

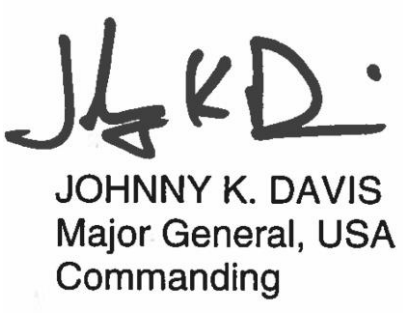
FORT KNOX REG 190-13, Dated 1 April 2022

Distribution Restriction Statement
This regulation contains technical or operational information that is for official Government use only. Distribution is limited to US Government agencies.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Military Police

Fort Knox Physical Security Program



Summary. This regulation establishes the Fort Knox Physical Security Program.

Applicability. This regulation applies to Department of Defense (DoD) employees, contractors and all units, organizations or activities assigned, attached or tenant to Fort Knox. This regulation does not authorize methods of operation or requirements outlined or specified by higher command to be changed in any manner. In the case where this regulation may conflict with a higher command's requirement or regulation, the more stringent standard of the two will apply. Questions concerning the applicability and interpretation of contents should be referred to the Directorate of Emergency Services (DES) (ATTN: Physical Security Office).

Proponent. The proponent for this regulation is the Physical Security Office, DES, Fort Knox, KY 40121.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of the Installation Physical Security Office, DES. Commanders (CDRs)/Directors (Dir)/ Facility Managers (FMs) will not deviate from or supplement this regulation.

Suggested Improvements. Users are invited to send comments and suggested improvements on Department of Army (DA) Form 2028, Recommended Changes to Publications and Blank Forms, directly to Director, DES (ATTN: Physical Security Office, (IMKN-ESS).

Distribution. This publication is available in electronic media only, and is limited for official Government use only.

Contents (Listed by paragraph and page number)

Chapter 1
General

1-1. Purpose. This regulation provides Commanders, Directors, and Facility Managers (CDRs/DIRs/FMs) with guidance and assistance for developing, executing, and maintaining an effective physical security program. For the purpose of this regulation, Fort Knox includes all units and facilities on Fort Knox Property or any standalone facilities. This regulation is intended to provide additional physical security guidance otherwise not covered in existing Army Regulations and directives. Any Army regulations or DOD manuals, instructions or directives take precedence over this regulation. Any conflicting information contained in this regulation should be brought to the attention of the Installation Physical Security Officer (IPSO).

1-2. References. Required and related publications and prescribed and referenced forms are listed in Appendix A.

1-3. Explanation of Abbreviations and Terms. Abbreviations and terms used in this regulation are explained in the glossary.

1-4. Installation Physical Security Office (IPSO). The IPSO's responsibilities include, but are not limited to:

a. Assessing the installation's physical security needs by conducting physical security surveys, risk analysis, staff assisted visits, and inspections.

b. Identifying Physical Security requirements with US Army Corps of Engineers during the planning, design, and construction of new construction, renovations, modifications, or lease acquisition.

c. Providing technical support for threat assessments.

d. Monitoring resource management of the installation Physical Security program.

e. Providing guidance and training if requested for personnel with duties related to Arms, Ammunition, and Explosives (AA&E) and assigned physical security managers of tenant units.

1-5. Disciplinary Actions

a. Disciplinary action may be imposed on persons in violation of the provisions and requirements of applicable governing laws and/or regulations.

b. Violations of federal laws may provide a basis for prosecution. Under the provisions of the Assimilative Crime Act, persons not subject to the Uniform Code of Military Justice (UCMJ) may be prosecuted by the US Magistrate and the US District Court, as appropriate, for violation of any state or federal laws, committed entirely or in part on Fort Knox.

1-6. Security of Unclassified Government Property (Sensitive and Non-Sensitive). Physical Security is a critical part of the DoD Force Protection Program. A successful Physical Security and Force Protection program cannot be achieved without command emphasis and involvement. The IPSO recommends that all construction sites on the installation take security and physical measures to eliminate theft, damages and trespassing during all military construction projects. IAW AR 190-51, 3-21, all Facility engineering supply, construction material storage areas, and industrial and utility equipment will be secured and protected. A risk assessment must be completed prior to construction using DA PAM 190-51. After the risk assessment see below for what measures must be completed. The Mission Installation Contract Command (MICC) will ensure the risk assessment requirement is in all military construction projects contracts. All equipment or property stored in the same location, valued at $500,000.00 and above will be secured IAW AR 190-51, 3-12, regardless of CIIC, unless otherwise specifically directed by AR 190-51.

1-7. Responsibilities

a. Garrison Commander (GC). The GC will ensure physical security regulatory requirements are implemented on Fort Knox in support of this regulation to include identifying and prioritizing physical security resource requirements based on threat, vulnerabilities, regulatory guidance, and command directives.

b. Directorate of Public Works (DPW). The director will:

(1) Establish a formal process to ensure physical security design criteria are considered for proposed construction projects in compliance with Army military construction policy.

(2) Maintain an overview of the physical security design program and activities pertaining thereto.

(3) Ensure IPSO is notified of all new and renovation construction projects. This notification will be early and be prior to plans being developed at conceptual phase of a project.

(4) Request from the IPSO a security engineering survey. This survey is an on-site assessment of physical security engineering requirements. Security engineering surveys will be performed when planning new construction or renovations to facilities where there are likely to be physical security requirements. Security engineering

surveys may also be requested by the project manager (PM) or equivalent security officer to evaluate existing security.

c. Directorate of Emergency Services (DES). The DES will:

(1) Assess installation physical security needs by conducting a physical security survey every three years ensuring the garrison and senior commander approve the survey. Also, annually review and approve in writing the Physical Security Plan (PSP) and ensure the PSP is exercised annually.

(2) Oversee the operation and maintenance of the Fort Knox Integrated Commercial Intrusion Detection System (ICIDS).

(3) Ensure a Physical Security Council (PSC) is convened as needed. Work through the PSC to train, coordinate and improve the Installation Physical Security Program. Ensure Senior Commanders are briefed on critical physical security issues/findings.

(4) Ensure Crime Prevention programs complement the Installation Physical Security/Crime Prevention (PSCP) Program. Further, law enforcement security check plans will be coordinated with IPSO. LE will conduct security checks of facilities designated by IPSO and approved by director IAW Army Regulation (AR) 190-11/13.

d. Installation Physical Security Officer (IPSO). The IPSO will:

(1) Be appointed in writing by the Senior Commander. Serve as the single point of contact for all physical security matters and oversee the installation physical security program.

(2) Be a credentialed Physical Security Specialist (PSS).

(3) Co-chair the PSC with the Director DES and oversee the operation and maintenance of the Fort Knox Integrated Commercial Intrusion Detection System (ICIDS).

(4) With DES Director, ensure a Physical Security Council (PSC) is convened as needed. Work through the PSC to train, coordinate and improve the Installation Physical Security Program. Ensure Senior Commanders are briefed on critical physical security issues/findings.

(5) With DES Director, assess installation physical security needs by conducting a physical security survey every three years ensuring the garrison and senior commanders approve the survey. Also, annually review and approve in writing the physical security plan.

(6) Communicate with units directly and through the PSC for any updates to inspection schedules, regulations, training or changes from higher headquarters.

(7) Set the physical security inspection schedule and approve any requested changes to inspection schedule.

e. Brigade (BDE)/Battalion (BN)/Directorates (DIR) must:

(1) Develop a Physical Security Plan (PSP), IAW AR 190-13, 2-8 and App C and provide a copy to the IPSO for inclusion into the Installation PSP, ensuring MEVAs are established within their command. Ensure a barracks physical security plan is developed and implemented, IAW AR 190-13, App D.

(2) Appoint in writing a Physical Security Officer/manager at their level to oversee the Command's physical security mission. This person will be a Sergeant or above, General Schedule (GS) 6 or above at the BDE/BN/DIR level (IPSO recommends SSG or above). BN/DIR PSOs will attend all Physical Security Council (PSC) meetings.

(3) Every three years, ensure that all units/facilities/sections complete a Risk Analysis worksheet DA Form 7278 IAW AR 190-51 and DA PAM 190-51.

(4) Ensure each unit/section/facility within their command or footprint develop and implement a Physical Security SOP which includes security responsibilities for the receipt, utilization, and accountability of government AA&E/sensitive items property. Further, the SOP will include the following subjects: Key Control, Building Security, Emergency Actions, End of Day Checks, Motor Pool, Tool Room, Seals, Crime Prevention, Weapon/Key/Sensitive Item security training and ICIDS Failures.

(5) Establish periodic informal inspections of their subordinate units/activities conducted by unit PSO.

(6) Protect, assess and account for property in accordance with regulatory requirements.

(7) Ensure personnel directly responsible for key control, AA&E and sensitive items are trained on all physical security requirements.

(8) Ensure personnel assigned and or directly responsible for Physical Security are trained on all physical security requirements.

(9) Ensure all units/section that have AA&E have appointed an Arms Room OIC or NCOIC or Department of Army Civilian (DAC) in writing.

(10) Approve and submit an annual restricted area and MEVA memorandum to the physical security office.

f. Company Commanders/Facility Managers

(1) Appoint in writing an AA&E OIC/NCOIC/DAC, if applicable. Ensure they are

trained on all physical security requirements.

(2) Appoint in writing a Unit/Facility/Division Level Physical Security OIC/NCOIC/DAC in the rank of Sergeant/GS-6 and above. Ensure they are trained on all physical security requirements.

(3) Appoint on orders a Key Control Officer and Custodian. Ensure they are trained on all physical security requirements.

(4) Ensure the Unit/Facility Physical Security SOP includes (if applicable): Arms Room, Armor Prerequisites, Motor Pool, Tool Room, Seals, Weapon/Key/Sensitive Item security training, Emergency Action Plans, ICIDS, ICIDS Failures, Weapons Immersion, Privately Owned Weapons (POW) and Key Control.

(5) Ensure all unit armors are trained on AA&E procedures, all Key Custodians are trained on Key Control and individuals within the command are trained on weapon, key and sensitive item security.

(6) Ensure SF 701 and 702 are implemented and used.

(a) SF 701, End of Day Checks, a separate SF 701 will be used for each division or section with-in a unit or facility.

(b) SF 702 Security Container Check Sheet will be used on all AA&E facilities, safes and anywhere a security check is required by regulation. The personnel opening AA&E or safe will initial the SF 702 each time the AA&E or safe is opened and secured. Further, any security checks will be annotated on the SF 702.

(7) Ensure all Armors, Physical Security Officers and Key Custodians have been interviewed, trained and had a completed background check. The favorable background check and training must be stipulated on the memorandum requesting access to AA&E facilities through the IPSO.

g. Unit Physical Security Officer (PSO) will:

(1) Be appointed in writing by the BDE/BN/DIR/Company (Co.) level (i.e., Co, Battery, Troop, Flight) CDRs, and DIR/FM.

(2) Meet the requirements of AR 190-13, para. 3-1.

(3) Be trained on all physical security requirements.

(4) Have a favorable background check, training and commander’s interview completed prior to assuming duties.

(5) Coordinate physical security inspections through the unit S2/S3 and the IPSO,

624-1713/4780/4788/1236. Coordinate between IPSO and the unit to be inspected, gathering all documents, SOPs, orders and points of contact for IPSO. Be present at all inspections with in the command/directorate.

(6) Conduct semi-annual physical security inspections of subordinate units and maintain inspection records on file until the next scheduled inspection. Review physical security and crime prevention inspection results and recommend improvements to the CDR/DIR.

(7) Provide annual physical security and crime prevention briefs to command headquarters and subordinate commands.

(8) Attend all Physical Security Council (PSC) meetings (BN/DIR PSO only). Ensure commands adhere to PSC guidance and changes or updates in policy.

(9) Advise CDR/DIR on information which may impact crime trends. Conduct annual refresher training on all aspects of the physical security plan/SOP to all personnel with-in the command. Include the following subjects: (If Applicable) Arms Room, Motor Pool, Tool Room, Seals, Crime Prevention, Weapon/Key/Sensitive Item security training, Crime Prevention, Emergency Action Plans, Power Outage Plan and Key Control.

(10) Ensure Staff Duty Officer (SDO) and/or Staff Duty Noncommissioned Officers (SDNCO) use SF Forms 701 and 702 and conduct random End of Day checks of AA&E, barracks, unit areas, equipment storage areas, motor pools and parking lots during hours of darkness and weekends. Staff Duty Officer/SDNCO journals will be maintained on file for a minimum of 90 days.

h. Arms Room Officer, Officers in Charge (OIC), Noncommissioned Officers in Charge (NCOIC) will:

(1) Be a commissioned officer, warrant officer or an E-5 and above, or a DA civilian equivalent. Sign for on hand receipt all AA&E and sensitive items stored in the Arms Room.

(2) Be appointed in writing by the CDR/DIR.

(3) Be trained on all physical security requirements.

(4) Have a favorable background check, training and commander’s interview completed prior to assuming duties.

(5) Familiarize themselves with references in Appendix A of this regulation. Note: supply personnel will not be appointed as Arms Room Officers (ARO).

i. Unit Armorers will:

(1) Primary and alternate armorers will be appointed in writing by the CDR/DIR.

(2) Be trained in AA&E procedures, physical security requirements and key control.

(3) Have a favorable background check, training and commander's interview completed prior to assuming duties. Personnel pending non-judicial punishment, administrative separation due to adverse actions, pending or convicted of domestic violence in violation of the Lautenberg Amendment, or have been determined to be medically or mentally unfit for duty by medical authorities are prohibited from assignment.

(4) Be familiar with applicable references in Appendix A of this regulation.

(5) Be strictly prohibited from conducting or participating in monthly inventories and will serve in an observation role only.

j. AA&E and Admin Key and Lock Custodians will:

(1) Be appointed as a primary or alternate AA&E and/or Admin Key and Lock Custodian in writing by the CDR/DIR.

(2) Have a favorable background check, training and commander's interview completed prior to assuming duties.

(3) Be familiar with applicable references in Appendix A of this regulation. Be trained in Key Control procedures and not have unaccompanied access to AA&E.

(4) Be trained on all physical security requirements and Key Control Procedures.

k. Inventory Officer for Monthly Sensitive Items Accountability will:

(1) Be selected by the CDR/DIR and not be flagged or under any adverse investigation.

(2) Be strictly prohibited from conducting consecutive monthly inventories.

(3) Physically account for and inventory all AA&E, POWs and sensitive items stored in the arms room by serial or lot numbers.

(4) Be a Commissioned, Non-Commissioned or Warrant Officer.

Chapter 2
Physical Security Planning

2-1. Risk Analysis

a. Commanders/Facility Managers (FM)/Unit PSO will conduct a risk analysis of their assets IAW AR 190-51 and DA Pamphlet 190-51 to determine the appropriate risk level of protection.

b. Risk analysis will be conducted by the Unit PSO and CDR/DIR/FM:

(1) When a unit or activity is activated.

(2) When a unit permanently relocates to a new site or facility.

(3) When no formal record of a previous risk analysis exists.

(4) At least every three years.

(5) During the planning stages of new facilities, additions, and renovations to facilities.

(6) When an asset is compromised or as needed.

c. Physical Security Officers must determine the level of physical and security protective measures required to mitigate the indicated risk level IAW AR 190-51.

2-2. Physical Security Plan (PSP)

a. BDE/BN/DIR will develop a PSP IAW AR 190-13, para 2-8, Appendix C and integrate PSPs with the unit Antiterrorism/Force Protection program.

b. BDE/BN/DIR must coordinate and establish the PSP with subordinate units and activities. Physical Security Plans will:

(1) Establish procedures and responsibilities and address the protection of all buildings, vehicles, equipment and property with-in the command or directorate.

(2) Establish contingency procedures.

(3) Identify changes in requirements at higher Force Protection Conditions (FPCONs).

(4) Ensure subordinate and tenant activity SOPs integrate with and complement their PSP.

(5) Be reviewed annually by the next higher command. Validated by IPSO during the annual inspection process.

(6) Physical Security Plans must include the basic requirements of Appendix C, AR 190-13. Some areas of Appendix C may not apply to all commands.

2-3. Installation Physical Security Inspections. Physical security inspections are a formal recorded assessment of physical security procedures and measures implemented by a unit or activity to protect its assets.

a. Physical Security Specialists (PSS):

(1) Will not engage in illegal or dangerous conduct to demonstrate security deficiencies or weaknesses observed during an inspection.

(2) May conduct announced and unannounced inspections.

(3) IAW with AR 190-13, 2-15e, PSS are credentialed personnel and will be granted access to facilities, assets, records and other information on a need-to-know basis consistent with PSS clearance level.

b. Physical Security inspections will be conducted:

(1) In accordance with AR 190-13, para 2-15 and as deemed necessary by the Director DES and the IPSO.

(2) When a MEVA, unit, or activity is activated.

(3) When a record of a prior physical security inspection does not exist.

(4) When a unit or activity changes in a way that may affect current PSPs, and there is a report of significant recurring criminal activity.

(5) Every 18 months for conventional arms and ammunition storage activities.

(6) Every 18 months for critically sensitive activities/facilities, and dining facilities.

(7) Every 24 months for MEVAs other than those listed in paragraphs (5) and (6) above.

c. Courtesy inspections will not be conducted in lieu of formal inspections or with-in 90 days of announced inspections.

d. Request for changes to dates of a scheduled inspection must be submitted by the organization’s battalion commander, director or equivalent in their chain of command and forwarded to the IPSO for approval.

e. Installation Physical Security Office PSS will provide Unit Physical Security Managers with a daily progress report. Upon completion, the IPSO PSS will provide a formal out-briefing of inspection results to the CDR/DIR or representative. All completed reports will be forwarded to the unit higher command.

f. Discretion to make on-the-spot corrections lies with the IPSO PSS.

g. Commanders/DIRs must immediately correct or implement adequate compensatory measures until the deficiency can be corrected. The sole submission of a work order is not considered a compensatory measure.

h. IAW with AR 190-13, all inspections and check list will be completed using Security Manager System-Counter Measures (SMS-CM).

i. DA Form 2806-1-R

(1) Units or activities which receive a “Not Adequate” rating on an Installation Physical Security Inspection will submit a Corrective Actions Plan (CAP) in memorandum format to the IPSO within 45 calendar days of receiving the official inspection results. The CAP must be received before a re-inspection can be conducted. Re-inspections will be conducted no later than 180 days from the date of initial inspection without the approval of the IPSO.

(2) The corrective action memo must identify the corrective actions taken, compensatory measures implemented, or both to address findings on the survey, inspection or vulnerability assessment.

(3) The IPSO will electronically forward inspection results to the inspected unit within 30 calendar days, and an out-brief within 30 calendar days after the inspection. Copies of physical security inspection reports will be provided to the higher headquarters of the unit inspected.

j. Units and activities must retain inspection reports until their next scheduled inspection.

k. Units receiving an ‘Not- Adequate’ must address and fix all deficiencies no more than 90 days after inspections. Commanders or responsible officials may decide to assume risk by not changing security measure deficiencies, however mitigating measures will be implemented to reduce the risk as low as possible. Those security measures deficiencies or procedures must be officially recorded on a DA Form 2977, Deliberate Risk Assessment and submitted to IPSO. (Examples of physical measures are security lighting, fences or alarms. While security measures are procedures such as after hour checks, key control and inventories.)

(1) AR 190-13, paragraph 2–3. Identifies the Security criteria deviation process and the difference between Waivers, Limited exceptions and Permanent exceptions.

(2) The asset owner is responsible for initiation of a Security Criteria deviation for any physical security deficiencies that are unable to be fixed.

(3) The waiver must be initiated in OPMG Data Integration Net (ODIN) at **https://army.deps.mil/army/sites/PMG/ODIN.** This process is started by assigning a "requestor" in ODIN and coordinating all efforts with IPSO. Once the requestor has access to ODIN they will submit and track the waiver.

(4) Installation Physical security officer is the installation Point of Contract for requesting user access on behalf of the asset owner and can provide assistance with the formal submission process.

(5) Installation Physical Security office will provide training information for all new requestors.

2-4. Inspection Requirements

a. Inspection ratings will be recorded via Security Management System-Counter Measures (SMS-CM) web based database. Inspections will be rated as either Adequate or Not Adequate. A rating of Not Adequate will be given based on:

(1) One major deficiency. Major deficiencies are identified in SMS-CM as 'critical'.

(2) Lower than 80 percent as calculated by SMS-CM with-in a functional area. Deficiencies are classified as areas lacking or missing certain Physical Security Program requirements; however, the deficiencies are not classified as serious enough to cause immediate stoppage or closure to the affected area, (e.g. motor pools, AA&E, etc.). Examples of deficiencies would include, but are not limited to failure to keep necessary regulations on hand and improper or missing memos.

(3) A recurring correctable deficiency(s) from a previous inspection.

(4) IPSO with input from PSS determines there is no viable physical security program established in a facility or unit.

(5) A no show at an approved, accepted and announced inspection date and time.

b. Re-inspections

(1) Will only be conducted after a CAP is received and approved by the IPSO.

2-5. Posting of Restricted Area Signs

a. Signs or notices will be posted in conspicuous and appropriate places to identify the site as a restricted area except when such action would tend to advertise an otherwise concealed area. Announcement of the site as restricted will include posting signs at each entrance to the site and on perimeter fences or other boundary material.

b. Signs will be positioned to avoid concealment of an intruder or obstruct visual assessment by friendly forces. Failure to post conspicuous signs and notices to give persons approaching a restricted area actual knowledge of the restriction may hamper any resulting legal procedure.

c. Signs will be provided by IPSO and a work order submitted by the unit to DPW to place the sign(s) in the proper place.

d. Sizes of signs: Restricted Area-Outside/Fence line, 24”x 36”; Inside, 18” x 24”.

Chapter 3
Arms, Ammunition and Explosives (AA&E)

3-1. Arms Room Standing Operating Procedures (SOP). Commanders, DIRs, and FMs are responsible for establishing an SOP for the protection and accountability of AA&E/sensitive items stored in their AA&E facilities. Standard operating procedures must be reviewed by IPSO annually and include:

a. Current CDR/DIR/FM signature.

b. Duties for:

(1) Primary and alternate armorers.

(2) Unit Arms Room Officer (ARO).

(3) AA&E Key and Lock Custodians.

(4) Inspecting officer when conducting monthly Property Book Office procedures.

c. Soldier's responsibility for AA&E and sensitive items during operational and field training conditions.

d. Security of AA&E stored or mounted on vehicles and aircraft.

e. Reporting serious incident reports (SIRs) IAW AR 190-45, chap. 9 and AR 190-11.

f. Reporting procedures of actual, suspected loss or recovered AA&E, and sensitive items losses. The DES must be immediately notified upon discovery of any loss IAW AR 190-11.

g. Security of AA&E and sensitive items for Soldiers medically evacuated during training.

h. Specific procedures for posting armed guards (with firearm and like ammunition) in cases of Integrated Commercial Intrusion Detection System (ICIDS) alarm failures or elevated FPCONs. Guards must sign an acknowledgement statement of their assigned duties and responsibilities IAW AR 190-14 and must be additionally briefed on; their responsibilities, rules of engagement, and the use of force.

i. Use and completion of required forms, (e.g., Weapons, Ammunition, Sensitive Items, and Key Count/Inventory; Request for IDS PIC, DA Form 3749, MAL, etc.).

j. Issuing procedures of AA&E and protection of AA&E while in transport, field exercise and ranges.

k. Training programs for Key Control, Armorers, Weapons Security and AA&E alarms testing.

3-2. Arms Room Consolidated Storage Agreements. When more than one unit/activity share the same facility for the storage of AA&E, a Memorandum of Understanding (MOU) will be prepared and signed by all associated CDRs unless the host is appointed in writing by the BDE/BN CDR. The Host CDR (HC) will have overall responsibility for security of the storage facility. The MOU will include:

a. Maximum quantities of AA&E authorized to be stored per tenant unit.

b. Physical safeguards required for use, (e.g., racks, locks, etc.).

c. Responsibility for frequency of issuing/receiving, or conducting physical inventories and reconciliations.

d. Reporting procedures for loss/stolen equipment and sensitive items IAW AR 190-45 and AR 190-11, 1-16, 2-9, 8-2, 8-3 and App E.

e. Key and lock control procedures.

f. Hand receipt procedures for receipt and issuance of AA&E/sensitive items.

g. Risk categories of items authorized to be stored.

3-3. Arms Room Security Lighting. Interior and exterior lighting is required for all AA&E facilities. Light switches will be inaccessible to unauthorized personnel and entrance/exit doors will be properly illuminated.

3-4. Arms Racks and Security Containers

a. Arms racks and security containers used to secure AA&E/sensitive items will be General Service Administration (GSA) approved National Stock Number (NSN) or Tank-Automotive Command (TACOM) certified.

b. Fabricated arms racks, containers, and metal standard issue wall lockers require approval and certification from the local US Army TACOM, Life Cycle Management Command office. Certification numbers issued by the Logistics Assistance Representative (LAR) will be visibly displayed.

c. Arms racks/containers will be locked with approved secondary padlocks and containers weighing less than 500 pounds will be fastened to the structure or in groups totaling more than 500 pounds, IAW AR 190-11 para 4-2.

d. Chains securing racks/containers will be galvanized steel of at least 5/16-inch thickness or of equal resistance required to force, cut, or break an approved low security padlock.

3-5. AA&E Locks and Keys. Recommend AA&E keys placed on one ring that is welded or locked to prevent keys from easily being lost or replaced. Key custodian will facilitate any key replacement. If any keys/locks are lost an inquiry will be conducted by the key custodian and a written memo will be kept on file until the next semi-annual inventory. Keys will be signed for from the unit key custodian or staff duty if authorized by unit PSP or SOP. All locks will be secondary low security key retaining padlocks.

3-6. Security of Armorer Tools. Armorer tools stored inside an arms room will be secured in locked containers using DoD approved secondary padlocks. Hammers, crow bars, bolt cutters, and other large tools will not be left unsecured at any time and will be secured in the supply room IAW AR 190-51, App E.

3-7. Security of Non-AA&E Items

a. In the absence of other secure areas, CDRs/DIR/FMs must authorize in writing the storage of non-AA&E items (e.g., bayonets, lasers and combat optics and other high value items) in an arms room equipped with ICIDS. These items should be secured in wall lockers or other locked containers.

b. In such cases non-AA&E items will be accounted for on DA Form 2062 by nomenclature, quantity, and added (in writing) on the monthly PBO sensitive items "working copy" report by nomenclature, quantity, and serial number if applicable.

c. Serial numbers not embedded or affixed to/on equipment such as NVDs, lasers, and other combat optics or which have identity number plates tending to become separated from devices will be permanently affixed by an alternate means, (e.g., engraving, permanent stamping, etc.).

d. Night vision devices, lasers, and optics will be secured with-in a double barrier system and accounted for on the daily inventory. Armorers will conduct a visual count of all NVDs upon first accessing the arms room for the day. The arms room does not have to be accessed solely to conduct the count. The visual count will be conducted by opening each case and viewing the device, or having the NVDs stored in a locked container with a protective seal control IAW 5-6 of this regulation. Results of the visual count will be recorded on DA Form 2062 and retained on file for 90 days.

(1) Issuance Procedures. Night vision devices will be issued using the same procedures as those used for weapons IAW DA Pam 710-2-1, paragraph 5-6d.

(2) Night vision device inventory requirements.

(a) Will be included in the monthly serial number inventory.

(b) Will be inventoried by serial number in conjunction with serial number inventories of weapons/sensitive items.

(3) Field Storage

(a) Individual Soldiers will be responsible for their assigned NVDs and will ensure they remain in their possession until returned to the arms room.

(b) If the NVDs cannot be kept with the Soldier, they will be stored in a central location under constant surveillance by a guard.

(4) Transportation

(a) When not physically issued to Soldier, NVDs in transit will be inventoried prior to shipment, stored in a locked sealed container, and re-inventoried upon arrival.

(b) Missing or lost NVDs will be reported to MP Desk and IAW AR 190-45.

3-8. Privately Owned Weapons (POWs)

a. Personnel residing on Fort Knox are required to register their POWs with the DES IAW Chap 16.

b. Commanders will:

(1) Ensure armorers account for and inventory POWs and ammunition secured in unit arms rooms both on DA Form 2062 daily and during monthly sensitive items.

(2) Ensure DA Form 3749 is issued for each POW secured in an arms room. Each POW will be inventoried in conjunction and at the same frequency as military weapons.

(3) Establish limits on quantity and type of POW ammunition stored in the arms room based on space availability and safety considerations IAW the unit's current ammunition license.

(4) Ensure operations/procedures/inspections are conducted IAW AR 190–11, 190–13, and this regulation to ensure proper storage and control of POWs, ammunition and war trophies.

(5) Ensure they are familiar with and adhere to all directives in AR 190-11 and POWs are registered IAW AR 190-11.

(6) Post applicable local regulations, state and local law information on ownership, registration, and possession of weapons and ammunition on unit bulletin boards.

3-9. AA&E Facility Security Checks (Refer to AR 190-11, 4-2a(3)(6)(7); e(1)(2), 5-2a(2), b(3))

a. AA&E Facilities with ICIDS coverage will have the following security checks:

(1) Category II-8 hours
(2) Category III/IV-48 hours

b. AA&E Facilities without ICIDS coverage will have the following security checks:
(1) Category II-8 hours, must add an armed guard
(2) Category III/IV-24 hours

c. Bulk Ammunition Facilities with ICIDS coverage will have the following security checks:
(1) Category I/II-24 hours
(2) Category III/IV-72 hours

d. Bulk Ammunition Facilities without ICIDS coverage will have the following security checks:
(1) Category I- 1 hour, must add armed guard
(2) Category II-2 hours, must add armed guard
(3) Category III/IV-48 hours

e. ARMAG (Portable) AA&E Facilities with ICIDS coverage will have the following security checks:
(1) Category II-IV-8 hours

f. ARMAG (Portable) AA&E Facilities without ICIDS coverage will have the following security checks:
(1) Category II-IV-8 hours, must add an armed guard

Chapter 4
AA&E Administrative Requirements

4-1. Personnel Evaluation Screening (DA Form 7708). Personnel Evaluations must be:

a. Completed prior to assignment as a unit armorer, Key and Lock Custodian, or personnel involved in the control, issue, and receipt of AA&E.

b. Maintained on file in the arms room as long as the person is authorized those duties. Personnel will be re-screened every three years. Ensure SSNs are protected or removed prior to posting.

c. Reviewed and documented annually by the certifying official and repeated every three years or when a new commander/director assumes command.

d. Digitally signed by the commander and emailed to DES Records section for back ground check. DES will only accept the signed form from a senior leader of the command or the Unit PSO. When completed the form will only be emailed back to the same unit senior leader or PSO who submitted.

4-2. Property Book Officer (PBO) Monthly Sensitive Items Inventories

a. Units will use the current property book sensitive items listing to conduct monthly weapons/sensitive items inventories IAW para 6-4, AR 190-11. A two year history of these inventories “working copy” (signed) will be retained in the arms room (four years if discrepancies were noted or reported).

b. Personnel designated by the commander (Officer, NCO, Warrant Officer, or DoD Civilian appointed by the responsible officer) will conduct inventories.

(1) Consecutive monthly inventories cannot be conducted by the same person.

(2) Unit armorers are strictly prohibited from conducting or participating in inventories.

(3) The Inventory Officer/NCO must review all supporting documentation for items not physically present during the inventory. The Inventory Officer/NCO will record the results of the inventory on the “working copy,” and print, sign, list rank, and date the property book/ sensitive items listing on the date the arms room weapons/sensitive items inventory was completed. If the inventory exceeds a day, the Inventory Officer/NCO will list the date the arms room inventory was completed.

c. The disposition of weapons and sensitive items not present for inventory will be recorded adjacent to the item’s serial number. The following codes are recommended to record the disposition: (S/O) Signed Out, (M) Maintenance, (LT) Lateral Transfer, or

(T/I) Turn In. Armorers must provide documentation for items not physically present during the monthly sensitive items inventory.

d. Serial number inventories must be conducted of AA&E (including POWs and ammunition), military ammunition by lot number, bayonets and any other items authorized by the CDR stored in the arms room.

e. Sealed containers will be checked for signs of tampering and inventoried by validating the protective seal number against the memo posted on the exterior of the container. The Inventory Officer/NCO will record "as validated by protected seal#_____," adjacent the line item number (LIN). Physical inventories of container items will be conducted every six months.

4-3. Weapons and Sensitive Items Register. Each time an arms room is accessed and during joint change of custody between armorers will complete a count of all AA&E/sensitive items and record the results on DA Form 2062.

a. Arms Room OICs or commanders and armorers must conduct a joint inventory prior to applying protective seals to the locked container storing AA&E .

b. Record inventory on a memorandum signed by both parties which lists contents by type, nomenclature, quantity, serial number if applicable, and annotate the protective seal number used.

(1) Post a copy of the memo on the exterior of the locked/sealed container.

(2) The armorer conducting the daily inventory and the person conducting the monthly sensitive item inventory are not required to break the seal, as long as the memorandum is validated by matching the protected seal number listed on the memorandum against the locked/sealed container.

c. Personnel completing DA Form 2062 will:

(1) Compare the last inventory from the previous day with the first inventory of the present day. Any differences in the inventories will be reported immediately. Should any discrepancies be noted, a joint inventory must be conducted by the individual opening the facility and Arms Room OIC.

(2) Conduct a joint inventory as required if a change of custody of the AA&E/sensitive item storage container keys occurs.

(3) Ensure individuals accept responsibility for the arms room and the contents by printing their name and providing their signature in the DA Form 2062.

(4) Conduct and retain daily inventories of AA&E, to include additional items (e.g., spare barrels, ammunition, bayonets, military silencers/suppressors, and POWs) in the arms room as authorized by the CDR.

(5) Ensure the Total block indicates the total quantity of AA&E/sensitive items authorized by the Modified Table of Organization and Equipment (MTOE).

(6) Maintain a properly completed DA Form 2062 on file for 90 days.

4-4. Master Authorization List (MAL)

a. Armorers are responsible for establishing and maintaining a current hard copy of the MAL of assigned/unassigned AA&E/sensitive items stored in the arms room.

b. The MAL will list a Soldier's:

(1) Full name

(2) Rack number

(3) Equipment item serial number (i.e. weapon, NVD, scope, laser, etc.)

(4) Unit

c. Armorers will compare a Soldier's information against the MAL for proper issue of equipment and weapons. The MAL will not be displayed were it is visible to the public.

4-5. Department of the Army Equipment Receipt (DA Form 3749) or Service Equivalent Document for other services.

a. When a single item (weapon or sensitive item) is needed for issue to more than one individual, the armorer will prepare DA Form 3749 for each authorized item. Issue will be IAW DA Pam 710-2-1, para 5–6d (1) through (4), except that control sheet log (see form on Fort Knox home page) entries are required regardless of the time period for which the item is issued.

b. A Soldier's and CDR/FM or responsible officer signature will be completed in black ink. If a change of CDR/FM or responsible officer occurs, continue to accept the DA Form 3749 as long as the Soldier is assigned the weapon or equipment.

c. Lost DA Form 3749s will be reported to the CDR/FM immediately. Duplicated cards must be marked or stamped with the words, "DUPLICATE".

d. Each piece of equipment associated with a weapon, (e.g., optics, laser, etc.) will have its own weapon's card.

4-6. Weapons Issue and Turn-in Procedures

a. Individually assigned weapons/equipment issued, for under 24 hours, requires the turn-in of a DA Form 3749 (primary) or DA Form 2062 (secondary). For over 24 hours,

requires a weapons card and a weapons control log entry which will be retained in the arms room until weapons/equipment is returned.

(1) Assigned weapons will be drawn only by the person listed on the DA Form 3749. The armorer will validate the DA Form 3749 and the unit MAL match and the need for a weapon issue prior to issue.

(2) The turn-in of weapons will be conducted by the person issued weapon unless extenuating circumstances exist (e.g., medically evacuated during training exercise).

(3) Enter a single line entry with signature for each AA&E and sensitive item signed in or out.

b. For issue/return of crew-served weapons, DA Form 3749 (primary) or DA Form 2062 (secondary), and a weapons control log entry which will be retained in the arms room until weapons/equipment is returned.

4-7. Arms, Ammunition and Explosives Key and Lock Control

a. Only DoD approved low security, secondary, key retaining padlocks will be used to secure AA&E racks/containers and any container located in the AA&E facility.

b. High security padlock is the only authorized lock for securing entrance doors to AA&E facilities.

(1) Class 5 Armory (recommended) or Vault doors with combination locks that protect weapons and ammunition must meet the requirements of Federal specification FF-L-2937.

(2) Refer to the DoD Lock Program at the below web address: https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html

c. Use updated DA Form 5513, to record issue and receipt of AA&E storage facility keys.

d. The AA&E Key and Lock Custodian will:

(1) List the total number of keys for each lock by serial number and lock location.

(2) Update DA Form 5513 when keys/locks are added/removed from the AA&E facility.

(3) Complete all information including entering dates and times when issuing or receiving returned keys in the "Key Issue and Turn In" blocks.

(4) Maintain a completed DA Form 5513 on file for one year.

e. Security of AA&E keys and locks. The following procedures will be used by authorized personnel for the security of AA&E keys and locks:

(1) AA&E Key Custodian will issue the Armorer the AA&E keys upon request and verification of a need to access.

(2) Primary and alternate sets of keys will be maintained in separately locked containers with controlled access, alternate set of keys will be maintained by the higher headquarters. AA&E main door combinations will be held in a SF 700 sealed envelope at the higher headquarters. Both primary and alternate keys and combinations will be stored IAW 190-11, 3-8.

(a) AA&E keys to the locked container securing the arms room keys will be annotated on a separate DA Form 5513 and will not be included in the administrative key control system. Keys that open key containers will not be personally retained.

(b) AA&E keys and containers will not be stored in the same container with classified material; however, segregation in individual drawers is acceptable. Arms room/storage area keys will not be removed from the BDE/BN/CO area.

(c) Transfer of arms room keys between armorers will be recorded on a DA Form 5513 maintained in the AA&E facility. Also, during joint change of custody inventories the Daily DA Form 2062 will be signed by the armorer assuming responsibility.

(d) A single diagonal signature for multiple key/lock issues is prohibited. The DA Form 5513 will be completely filled out.

(e) Use of master/keyed alike locks (lock sets) is prohibited.

(f) Combination padlocks are prohibited.

f. Arms Room Key and Lock Custodian will ensure:

(1) A favorable background check (DA Form 7708) has been completed and a copy is maintained in the arms room.

(2) An inventory of AA&E keys is conducted initially, semi-annually or when there is a change of custody. Inventory results will be recorded on page 3 of DA Form 5513.

(3) Only appointed Key and Lock Custodian(s) are authorized to add or remove keys/locks from the AA&E/arms room key control system.

(4) The AA&E keys are issued to authorized personnel using DA Form 5513.

(5) A memorandum for record (MFR) will be completed when changes in the status of locks and/or keys occur.

(6) The alternate set of arms room keys (one key to each lock of the primary keys to include the maintenance key to the high security padlock maintained in sealed envelope or locked container) will be issued to the next higher S2 or headquarters on DA Form 5513 (one time initial issue). The arms room key box will be placed in a lockable container, (e.g., a safe). The unit/activity Key and Lock Custodian is solely responsible for conducting the semi-annual inventory of primary and alternate keys.

g. Lost or Stolen Keys and Locks. When keys or combination to a lock to secure main door to AA&E are missing or stolen, the Military Police (MP) and IPSO will be notified and a police report completed immediately. The affected arms room or area will be guarded until a new lock or combination is replaced, and changes recorded on all records and forms.

h. Replacement Locks. Replacement or reserve locks are authorized and must be part of the arms room key control system. Keys and locks will be issued to authorized personnel by the appointed AA&E Key and Lock Custodian. Locks will be secured in a locked container or secured to the chain to prevent removal of the weapon racks inside the AA&E facility.

i. The use of master or keyed alike locks is prohibited.

j. AA&E keys will NOT be taken off the installation.

4-8. Standard Form (SF) 700, Security Container Information Sheet. A SF-700 is required for AA&E facilities secured with an authorized mechanical combination lock or security containers and safes equipped with mechanical combination. Personnel completing the SF-700 will:

a. Complete Parts 1, 2 and 2a.

b. Enter the date the combination was changed.

c. List the first four persons, if applicable, to be notified in the event a container/vault is found open, unattended or compromised.

d. Detach Part 1 and post on inside of the vault door or drawer out of public view.

e. Mark Parts 2 and 2A with the highest classification stored in the container.

f. Complete and detach Part 2A and insert inside of Part 2. Insert Part 2 in an envelope. Store sealed envelope in a GSA approved safe at S2 or higher headquarters.

g. Change combination(s) when a vault or safe is put into service, annually, compromised, or there is a change in custodian(s) or personnel; reinitiate form 700 to reflect changes.

4-9. Standard Form 702, Security Container Check Sheet. The SF-702 will be used to record the opening and closing of AA&E facilities.

a. Heading information of each form must be completed.

b. AA&E security checks by guards or duty personnel will be recorded on the SF-702.

c. The SF-702 or SF-701, if applicable, will be maintained on file for a minimum of 90 days.

4-10. Department of Army Form 4604, Security Construction Statement

a. Arms room storage criteria for CAT II through CAT IV arms will comply with DODM 5100.76 and AR 190-11. Further, all AA&E storage facilities require a DA Form 4604-R, Security Construction Statement. DPW will validate the construction of all AA&E facilities have met all DOD and DA standards, prior to approving the DA Form 4604-R.

b. A Security Construction Statement will be issued by a qualified Directorate of Public Works (DPW) Engineer every five years and must be visibly affixed to an interior wall of the arms room.

c. Security Construction Statements are facility specific and will not be transferred to another facility.

4-11. Required Signage

a. Local and Kentucky firearms laws will be posted in a conspicuous area on the exterior wall of the arms room.

b. Intrusion Detection System Alarm Signs. A permanently affixed IDS alarm sign will be displayed near eye level by the exterior entrance door of each arms room vault.

c. Restricted Area Signs. An affixed "Restricted Area" sign per AR 190-13 will be prominently displayed on the exterior and by entrance doors of AA&E facilities.

d. Fire Control Symbols (Signs). Must be mounted and displayed IAW DA Pam 385-64.

e. Lautenberg Amendment Message. United States Code (USC) 18, Section 922(g)(9) Lautenberg Amendment to the Gun Control Act of 1968, effective 30 September 1996, makes it a felony for those convicted of misdemeanor crimes of

domestic violence to ship, transport, possess, or receive firearms, or ammunition. The amendment also makes it a felony to transfer a firearm or ammunition to an individual known or reasonably believed to have such a conviction.

(1) A copy of the Lautenberg Amendment Message as contained in Headquarters Department of the Army (HQDA) message dated 172023ZMay2002 will be posted on the exterior wall adjacent to the arms room entrance door.

(2) The message is directed to all personnel and states that personnel convicted of domestic violence will not be authorized to possess, carry or use firearms.

f. Risk Analysis. A risk analysis will be conducted of arms rooms and restricted areas every three years using DA Form 7278-R, Risk Level Worksheets. DA Form 7278-R will be maintained in the arms room and in unit/activity files until the next scheduled analysis.

4-12. Unaccompanied Access Rosters

a. Will be signed by the CDR/DIR/FM.

b. Will be posted and protected from public view inside arms room or AA&E facility.

c. Unescorted access to an arms room by persons not listed on the unaccompanied access roster is strictly prohibited.

d. Escorted persons will NOT be left unsupervised in the arms room at any time.

Chapter 5
Administrative Key and Lock Control (Non AA&E, refer to AR 190-51, App D)

5-1. Key and Lock Officer/Custodians

a. Key control and accountability must be established at all functional levels IAW AR 190-51, Appendix D. The Commander/Director will appoint a primary and alternate Key and Lock Officer and Custodian in writing for each unit or facility under their supervision.

b. Access rosters will be posted on the exterior of all key depositories. Appointment orders will not be used in lieu of access rosters.

c. Units with multiple key depositories which are located side by side require only one access roster as long as each key depository has been numbered. The access roster will reflect, “The following personnel have access to Key Box #1, #2, #3, etc."

d. Master keys/keyed alike set locks are not authorized unless specified in an Army Physical Security Regulation or approved by the IPSO. Exceptions are:

(1) Facilities with multiple exterior/entrance doors that open to the same interior, but open no other doors, offices or sections.

(2) Vehicle doors or compartments of the same vehicle. No keyed alike for multiple vehicles.

e. All keys and locks in use to secure government equipment will be included in a key control system.

f. A joint inventory of keys and locks will be recorded on DA Form 5513 and is required by the departing and incoming custodian whenever a change of custodian occurs.

g. Key control custodians will conduct an inquiry when any key or code is lost or compromised. Inquiries will be kept on file for 12 months and revealed to PSS during any inspections. The responsible commander/director will determine if the locks protecting the ‘lost key’ area will be replaced. Via a FLIPL process, the commander/director should seriously consider making the person at fault pay for any cost incurred for lost keys or re-coring of locks.

5-2. Key Control Register

a. Primary/alternate Key and Lock Custodians are responsible to ensure the key register is accurate and properly completed, and all keys are listed by serial number, location of their locks, and the total quantity of keys per lock. Use updated DA Form 5513 for this register.

b. Newly appointed Key and Lock Custodians will conduct an initial 100% key/lock inventory by serial number, and semi-annual inventories thereafter, IAW AR 190-51, Appendix D-6b. Inventories will be recorded on page 3 of DA Form 5513.

5-3. Key Depositories. Keys will be stored in a safe, lockable container, filing cabinet, or a key depository that is made of at least 26 gauge steel, equipped with a tumbler style lock and permanently affixed to the wall.

5-4. Locks

a. Only DoD approved low security padlocks will be used to secure government property. Locks will meet the following specifications:

(1) Keys shall be captive (key retaining/un-removable) in the cylinder when unlocked. Each padlock shall contain two keys.

(2) Marking. The markings "US" shall be .25 inch minimum size and will be located on either side of the padlock.

(3) Hardened shackle - will usually be stamped in the curve of the shackle.

(4) Heal and toe locking notches – with the lock in the open position there will be a notch on each end of the shackle. For approved locks refer to the DoD lock program: https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html

b. Department of Defense padlocks will not be cut/broken-off unless approved by the CDR or Key and Lock Custodian.

c. When a key to a padlock is lost or missing, an inquiry will be conducted and documented. The padlock will be replaced and recorded immediately on DA Form 5513 by the Key and Lock Custodian. If a door has a turn-key lock, the Key and Lock Custodian will call in a work order to DPW.

d. Commanders are permitted to assess financial liability for a lost key pursuant to AR 735-5.

e. All vehicles and fuel tankers, must be secured with the manufacturer's built-in locking device or an authorized padlock and chain/cable. Vehicles with universal built-in locking devices will be secured with a padlock and hardened steel chain of at least 5/16 inch in thickness.

5-5. Electronic Card Access Accountability

a. Access card control and accountability must be established at all functional levels IAW this regulation. The CDR/DIR will appoint a primary and alternate Access Control Administrator in writing. The primary Access Control Administrator is authorized to

approve, issue, and audit the personnel access control cards. The Key Control Custodian may be assigned as the Access Control Administrator.

b. The access control system and associated card stock will be maintained in a controlled area. Off limits to unauthorized personnel signs will be posted, and access to the area will be controlled with an access roster.

c. System card accountability and inventory will be conducted semi-annually. DA Form 5513 will be utilized to ensure accountability, issue, and return of an access card. DA Form 5513 will be maintained on file until the next inventory is conducted.

d. The access card control register will list card serial number, access location (i.e., building and room number), and total cards issued. If an access card does not have a manufactured serial number then the custodian will give it one. Cards cannot be engraved but can be written on with a permanent marker.

e. The Access Control Administrator may issue a master access card to the designated staff duty or Staff Duty NCOs utilizing a DA Form 5513.

f. System master access cards will be maintained and secured at all times. When a master access card is issued to staff duty personnel for after hour Soldier lock outs it will be signed out on DA Form 5513 and will be secured in a staff duty safe or container. If a master access card is needed for an after hour lock out, the staff duty personnel will notify the access card custodian or the unit First Sergeant and will make a staff duty journal entry. Journal entry should identify the date, time, and Soldier's information (i.e. name, floor, and room number). Only staff duty personnel in the rank of sergeant and above will use the master key, at no time will it be issued to the locked out Soldier. Staff Duty personnel will have the means to and verify room occupancy prior to opening a room.

g. Upon Permanent Change of Station (PCS) or Expiration Term of Service (ETS) from the unit, Soldiers must out process with the Access Card Administrator as part of unit clearing procedures in order to return and have their access card deactivated.

5-6. Protective Seal Control

a. Requirements. Protective seals are intended to be used as a supplement to verify the integrity of secured property. Protective seals will not replace the use of a padlock.

b. Issuing and Receiving Protective Seals:

(1) Commander/Director will appoint a Protective Seal Custodian in writing.

(2) Protective Seal Custodians will:

(a) Be issued protective seals by the S4 using a Seal Control Log or DA Form 5513. Old and unused seals will be returned to the Protective Seal Custodian to clear the seal registry and receive replacement seals if necessary.

(b) List and document seals received by serial number on a Seal Control Log Book or a DA Form 5513.

(c) Ensure initial seals are signed for by authorized personnel (record serial number(s), date, time of issue, and person receiving) on Seal Control Log. Notify the Protective Seal Custodian whenever a seal is destroyed or removed and complete a Memorandum For Record (MFR).

(d) Inventory of unused seals monthly (modified DA Form 5513 or equivalent form may be used).

5-7. Rapid Entry Key Boxes (Knox Boxes)

a. Emergency personnel such as police and firefighters will be provided card keys, key codes, lock combinations, keys, or other similar entry control devices needed to enter the perimeter of facilities. Emergency personnel are not authorized entry control devices to designated restricted areas. A single rapid-entry box can be utilized by all emergency personnel; there is no need to install separate boxes for each organization such as police and firefighters.

b. Entry control devices (for example, key, card, access code record) may be secured in a rapid-entry key box affixed to the exterior of the facility or adjacent to it to avoid emergency personnel having to maintain a large amount of entry control devices.

c. For Fort Knox Fire Department keys to rapid-entry boxes are secured in each fire truck and will be part of the daily truck inventory. Entry control devices maintained within the rapid-entry boxes will be inventoried IAW AR 190-51 by the concerned Key Custodian.

Chapter 6
Integrated Commercial Intrusion Detection System (ICIDS)

6-1. Integrated Commercial Intrusion Detection System (ICIDS) Alarms. All unit arms rooms and vaults will be protected by a minimum of two types of alarm sensors (balance magnetic switch and volumetric sensor such as passive infrared). An operational hardline phone will be installed in or just adjacent to the protected area. Cell phones will only be used as a back-up to communicate with the alarms monitor facility.

a. IAW AR 190-11, 4-2 e.(1), AA&E facilities without an operational ICIDS will be protected with armed guards 24 hours a day IAW with procedures in para 6-6 below. If a Director/Facility Manager has no ability to post an armed guard then they must acquire an Installation Service Support Agreement (ISSA).

b. The ICIDS is the only Army approved alarm system for AA&E/communications security (COMSEC) facilities on Fort Knox. CDRS/DIR/FM must ensure an updated ICIDS access memorandum is on file at IPSO. When personnel leave their command/section IPSO must be notified immediately to delete access in the system. POC for ICIDS is 624-1911.

c. Only those zones considered baseline services by IMCOM PS branch will be automatically monitored by DES. All other zones must enter into an ISAA with garrison and pay for above baseline services. (NOTE: Only AA&E facilities and IACP duress are considered baseline services.)

6-2. Alarm Activations

a. Alarm monitors will immediately contact the unit/activity point of contact(s) (POC) and dispatch MP patrols to all alarm activations triggered by unauthorized activity or access. If a facility alarmed asset is compromised or suspected to be compromised, a 100% inventory must be initiated immediately by the CDR/DIR/FM.

b. In the event of a "Duress Alarm" a MP patrol will be immediately dispatched to the scene in response to the alarm.

c. Observed or suspected breaches of an ICIDS alarmed facility during duty hours will be immediately reported to the unit CDR/activity PSO/S2/Security Manager, and IPSO. Security violations after duty hours will be immediately reported to the MP Station 624-6847 or 911. Authorized personnel must reset the alarm immediately if no violations are found.

d. The alarms monitor must record:

(1) Record name, rank, and title of the person responding to the security alarm incident.

(2) Notify and direct concerned unit/activity to have them standby until the MP have declared the area as safe. Unit personnel will conduct security and a 100% inventory check of the asset alarmed area.

(3) Record the name, rank, and title of the unit personnel conducting the security checks.

6-3. Alarm Tests

a. Units/activities with ICIDS protected storage facilities will conduct, record, and maintain monthly tests of the alarm system on a DA Form 4930 and keep on file for one year. The entire system, to include duress and motion sensors must be tested.

b. To conduct a test, the primary/alternate armorer or authorized access persons must provide the alarms monitor, 624-6016 with their name, building, and zone number.

c. The unit armorer or authorized access persons will take all directions from an alarm monitor in order to facilitate and complete the alarm test.

d. Ensure the motion sensors “walk lights” are disabled, if needed submit a work order to DPW to get these lights disabled.

6-4. Personal Identification Code (PIC). A current, accurate, ICIDS PIC Request memorandum signed by the CDR/FM is required to obtain a PIC for an ICIDS alarmed area.

a. All PICs will:

(1) Be issued to personnel requiring unaccompanied access to an ICIDS alarmed area or facility via the IPSO ICIDS POC at 624-1911. PICs will only be issued after an updated memorandum has been presented to IPSO verifying the back ground check and commander’s interview has been completed. These memorandums will be signed by the CDR/DIR/FM responsible for the alarmed area and updated every six months or upon a change of personnel. New memorandums must identify who is being added and/or removed. Points of contact will include duty and cell phone numbers.

(2) NOT be shared with other personnel, all violations will result in the installation personnel security officer being notified of a security breach and may result in further administrative actions.

(3) Be deleted immediately if no longer used, compromised, or suspected to be compromised.

b. Each CDR/DIR/FM must immediately notify the IPSO office if a PIC is compromised or suspected to be compromised.

c. Deleted PICs will not be reissued until CDR's/DIR's/FM's corrective action memorandum is received by the IPSO.

d. All personnel who are issued a PIC or access card from IPSO will out process the installation PS office located at building 298.

6-5. Security Breach of Arms Rooms/Sensitive Items Storage Areas. In the event of an actual breach of an AA&E/SI area:

a. Immediately notify the MP Station and the chain of command (COC).

b. Detain suspect(s) if possible until arrival of MP.

c. Notify the PMO immediately at 624-6847 or 911 and the Physical Security office at 624-1713. (NOTE: All zones will have telephonic communications ability in the protected zone, therefore IPSO highly recommends a dedicate hard line inside the zone.)

d. Immediately conduct a 100% serial number inventory of all AA&E/sensitive items.

e. Refer to chapter 8 of this regulation for lost and missing AA&E/sensitive Items.

6-6. ICIDS Failure Procedures

a. In event of a Category I or II, AA&E ICIDS failure, the unit/activity will immediately post an armed guard IAW with AR 190-11 and unit SOP. Guards must carry a weapon for which they are assigned and qualified. All guard personnel will be briefed on the Use of Deadly Force IAW AR 190-14.

b. In event of a Category III or IV, AA&E ICIDS failure or any other Non-AA&E ICIDS failure, a security check is required once every 24 hours by designated personnel (e.g., SDNCO/guard personnel). Checks will be recorded on a SF-702. Records of security checks will be retained in unit files for a minimum of 90 days.

6-7. ICIDS Work Orders

a. Units/activities must report problems and malfunctions of ICIDS sensors or systems to the IPSO at 624-1911. The Unit PSO will submit a detailed work order (to include problem description, date, building number, zone, and POC) for completion. Work order requests will be submitted to DPW as priority one.

b. An ICIDS technician will respond as soon as possible based on workload and priority of issued work orders.

c. The alarms monitor, MP desk supervisor or IPSO will direct units without operational ICIDS to comply with ICIDS failure procedures in paragraph 6-6 above.

d. Individuals with authorized access to the affected area must be present for technicians to complete repairs.

Chapter 7
Security of Unit Motor Pools

7-1. Commander (CDR)/Director (DIR)/Facility Manager (FM) and Contractor Responsibilities

a. Develop SOPs for controlling access and security checks to motor pools at all FPCON levels.

b. Establish procedures during operational hours:

(1) Control gate entry and exit at all times.

(2) Inspect all outgoing vehicles for a valid dispatch and equipment to deter and protect motor pool from pilferage, theft, and unauthorized removal of equipment and materiel at Risk Level III.

(3) Prohibit entry of all POVs into motor pools. Only exception will be for units engaged in deployment exercises with unit commander's written approval via unit SOP or memorandum.

(4) Motor pools will be properly secured during non-operational hours.

7-2. Requirements

a. An official risk analysis (DA Form 7278-R) is required for all tactical motor pools, to determine the level of physical protective and security procedural measures required.

b. Tactical vehicles will be parked in unit level motor pools when not in use. Exceptions include: deployments, ranges, training areas, or when authorized to park at rail shipping yards, or airfields.

c. IAW AR 190-51, tactical vehicles will be rendered inaccessible by locking the doors and making steering wheels inoperable with security chains/cables when not in use or in non-combat areas.

d. While in garrison, all tactical vehicles, trailers, gators, forklifts, etc., and lockable compartments will be secured with DoD approved locks when parked and unattended. Security chains will be at least 5/16th inch steel, unless manufacturer equipped cables are installed. Rear hatches (fuel dispensers) and top hatches (if applicable) will be secured if vehicle contains fuel. Locks will be DoD non-sparking padlocks. Master keys or keyed alike keys will not be used to secure vehicle steering wheels.

e. "Off Limits to Unauthorized Personnel" signs will be posted by all motor pool entrances. At Risk Level II, the motor pool will be designated as a Restricted Area and appropriate signs posted.

f. “No POV” signs will be posted by all motor pool entrances.

g. Tactical vehicle parking areas, storage containers and portable structures will be at a distance from the perimeter fence as determined by the risk analysis. At Risk Level II this requires 20 feet stand-off or as far as possible.

h. Unit security guard checks will be determined by the risk level.

7-3. Motor Pool Perimeter Fencing and Lighting

a. Motor Pool Perimeter fence. Fencing will meet the requirements AR 190-51, UFC 4-022-03 and UFGS 323113 drawing will be used as a guide.

b. Lighting. Vehicle parking areas, except those for empty trailers, will be lighted during the hours of darkness IAW UFC 3-530-01. Storage areas will be provided with operational interior/exterior lighting at all times during the hours of darkness. Unit PSO’s must submit a work order to the DPW for any lighting issues concerning vehicle parking or storage areas.

7-4. Key and Lock Control

a. Units/activities will establish SOPs for the control and accountability of keys/locks for vehicles, buildings, storage areas, and perimeter access points IAW AR 190-51, 3-11, App D.

b. Use of master keys or lock sets to secure vehicle steering wheels is prohibited.

c. Consolidated motor pools will designate one unit overall in charge of motor pool security, perimeter fencing, and lighting. A local SOP will be developed to address specific responsibilities.

7-5. Security of Tool Rooms. Commanders/Facility Managers will appoint a Tool Room Custodian in writing. Tools will be hand receipted to the custodian and signed out using DA Form 5519, Tool Sign Out Log/Register or an equivalent form. These forms will be maintained until all tools are returned and for 90 days there after.

a. Access rosters must be posted by the entrance to storage locations.

b. “Off Limits to Unauthorized Personnel” signs will be posted by entrances.

c. Storage areas will meet the security requirements IAW AR 190-51, Appendix B or full metal cage system in a secure building. Tool containers loaded on military vehicles will be secured when not in use.

d. Locks will be DoD approved low security and key retaining.

e. High dollar tools will be marked for unit ID and provided double barrier protection.

f. Mechanics will sign for their tool kits/box and will personally retain their key.

g. Standard Operating Procedures will address issues, receiving procedures and end of duty day reconciliations.

h. Tool kits and boxes will be secured when not in use.

Chapter 8
Lost/Stolen Military AA&E and Other Sensitive Items

8-1. General

a. Personnel who suspect or experience theft of government-owned AA&E items, will report their confirmed loss or theft immediately to the Fort Knox MP, 624-6847. An SIR must be completed and submitted IAW AR 190-45, chap 9 and all sections in AR 190-11, 1-16, 2-9, 8-2, 8-3 and App E, will be completed.

b. Losses and thefts occurring while participating in exercises off the installation, in a foreign country, or on any other installation, will be immediately reported by the responsible person to the appropriate MP and local authorities having jurisdiction.

c. Military Police desk supervisors will ensure all lost or stolen military arms are entered in NCIC. Ammunition and explosives will not be entered into NCIC.

8-2. Serious Incident Reporting (SIR). Sensitive items are those items identified in the Army Master Data File (AMDF) FEDLOG by a Controlled Inventory Item Code (CIIC) 1,2,3,4,5,6,8,9,N,P,Q,R,S,Y. When a weapon or sensitive item is lost or stolen, the senior ranking person assumes the position of on-scene CDR and must:

a. Notify the Fort Knox MP at 624-6847 within TWO hours of discovery.

b. Immediately notify the entire COC within a reasonable time frame upon discovering lost or stolen sensitive item.

c. Refer to AR 190-45 Law Enforcement Reporting for SIR procedures.

8-3. Types of Sensitive Items

a. Weapons.

b. AA&E.

c. All NVDs.

d. Military radios.

e. Automated Net Control Devices (ANCD)s/Signal Operating Instruction (SOI)s.

f. Communications Security (COMSEC) equipment (e.g., KY13, KY57, etc.).

g. Other items listed/coded in AMDF FEDLOG as a sensitive item.

8-4. Loss or Theft of AA&E Shipments. Transportation officers or designated representatives will report all information concerning the loss or theft of AA&E/sensitive item shipments to the Fort Knox MP Station.

Chapter 9
Transportation of AA&E and Sensitive Items

9-1. Arms, Ammunition and Explosives and Sensitive Item Serial Number Inventory Procedures

a. Commander's will conduct a 100% serial number inventory of all AA&E and sensitive items prior to the shipment of their equipment.

b. After the unit uploads deploying weapons, a responsible officer or NCO of the deploying unit and the rear detachment will conduct a 100% joint serial number inventory of all items remaining in the arms room.

c. Joint inventory results will be recorded on DA Form 2062 or on the unit's PBO hand receipt inventory form.

d. A copy of the joint inventory will be given to the rear detachment CDR, and a copy will be left inside the deploying unit's arms room. The deploying and rear detachment inventorying officer will print, sign, and date the inventory. Inventories will be retained until the forward deployed unit returns and both PBO hand receipts (forward deployed and rear detachment) have merged. The following month's inventory must reflect the merge.

e. The AA&E keys and locks will be transferred to the rear detachment AA&E Key and Lock Custodian using DA Form 5513 and the keys/locks will be re-issued to the armorer. Spare sets/alternate keys will be issued to the S2 using DA Form 5513.

f. Arms rooms that are not storing AA&E/sensitive items will be left unsecure with alarm in "access mode." The CDR will prepare and submit a memorandum stating "No AA&E/sensitive items are being stored" to the PIC code administrator in Building 298, 624-1911.

g. Stay Behind Equipment (SBE) weapons/sensitive items should be consolidated to the greatest extent possible.

h. Retain the original copy (list of deployed property issued out) of DA Form 2062 in the arms room and provide copies for deploying armorer.

9-2. Redeployment

a. Arms Room Activation:

(1) Submit an updated memorandum and request for ICIDS PIC to the ICIDS Administrator, 624-1911.

(2) Validate and update as necessary, arms room key and lock control systems during Key and Lock Custodian inventories.

(3) As applicable, change vault doors and safe combinations.

b. Items left in the arms room at the time of deployment MUST BE inventoried monthly and accounted for using proper PBO documents.

c. Returning weapons/sensitive items will be signed back in on the original copy of DA Form 2062.

9-3. In-transit Security of Unit AA&E/Sensitive Items. While on Fort Knox, use AR 190-11, 7-10 when transporting military AA&E. Military AA&E and sensitive items will remain in the possession of the person to whom it was issued at all times during training or transportation. The transportation of military AA&E and sensitive items in POVs is strictly prohibited.

a. Category I and II AA&E, will be escorted by an armed guard and in the custody of an Officer, WO, NCO (SGT or above) or a DAC (GS-5 or above).

b. Category III and IV AA&E, in the amounts of 16 weapons or more and/or 1000 rounds or more will be escorted by an armed guard and in the custody of an Officer, WO, NCO (SGT or above) or a DAC (GS-5 or above).

9-4. Shipments On/Off Fort Knox

a. All AA&E/sensitive items departing Fort Knox will be coordinated through the IPSO, LRC MASA and Installation Transportation Office and transported IAW the requirements of Department of Transportation (DOT) regulations, AR 190-11, DTRM 55-135, and DoD 4500.76M.

b. All AA&E/sensitive items transported during unit deployments will be provided double barrier protection; (i.e., locked container or inside a locked CONEX under armed guards.)

c. For additional information regarding movement of AA&E refer to AR 190-11, chapter 7.

9-5. Temporary Military Vehicles. Rental or leased vehicles procured by the government are considered temporary military vehicles and are authorized for use in the transportation of military weapons.

Chapter 10
Ammunition Supply Point (ASP)

10-1. Arms and Explosives (A&E) Bunkers. Non-nuclear missiles, rockets, AA&E listed in AR 190-11, Appendix B will be stored in approved igloo/bunker storage facilities at the Fort Knox ASP. All Category I-IV AA&E bunkers will meet all requirements of DoDM 5100.76, AR 190-11 and AR 385-64 to include: fencing, security lighting, ICIDS, key and lock control and entry control (refer to AR 190-11, Chap 5). Designated unit training bunkers must be approved by IPSO prior to being built or used.

10-2. Category (CAT) I and II AA&E Storage Facilities and Structures

a. Category I and II storage facilities and structures will be protected by IDS. Facilities without an operational IDS will have armed guards posted 24 hours a day to maintain; constant unobstructed observation of the storage structures, prevent any unauthorized access to the protected structure, and make known any unauthorized access to the structure.

b. Key and lock control will comply with AR 190-11 and AR 190-51, App D. Keys will NOT be personally retained.

c. Unaccompanied access rosters and background checks are required for each listed person.

d. A SF-702 is required to record entry, exit, and guard security checks.

e. After-duty hour guard checks are required on an irregular basis to ensure a pattern is not established. Retain guard records on file for 90 days.

10-3. Category III and IV AA&E Storage Facilities and Structures

a. Storage facilities and structures will be periodically checked by a security patrol as dictated by threats and or vulnerability of the facility. Category III and IV facilities protected by operational IDS will be checked once every 72 hours and facilities not protected by an operational IDS once every 48 hours.

b. Key and lock control will be maintained IAW AR 190-11 and AR 190-51, App D. Keys will NOT be personally retained.

c. Unaccompanied access rosters and supporting DA Form 7708s are required for each listed person.

d. A SF-702 is required to record entry/exit and guard security checks.

10-4. Security of Field Level Munitions Storage Areas (FLMSA)/Field Ammunition Supply Point (Refer to AR 190-11, 2-5)

a. Field Level Munitions Storage Areas will be:

(1) Designated by the CDR and used for temporary storage during field training events. After firing, the FLMSA may be used to reconcile the munitions prior to turn-in.

(2) Guarded by armed guards at all times regardless of FPCON and checked every four hours by unit personnel appointed by the commander.

(3) Secured with a high security padlock when not in use.

(4) Access will be strictly controlled. The two person rule applies to CAT I missiles and rockets.

(5) Temporary or permanent perimeter barriers to be positioned to prevent unauthorized entry into the storage area.

(6) Storage areas to be considered as restricted areas with proper signs posted.

(7) Armed guards to control access to CAT I through IV AA&E. When CAT I missiles and rockets are stored, the two person rule must be enforced. Guards will be equipped with a primary and alternate means of communications (i.e., a dedicated cell phone as a secondary means) and armed guards will be checked every four hours.

(8) Positive measures (i.e., security lighting or additional guards to be used during hours of darkness or reduced visibility).

(9) Accountability procedures to be established.

(10) Category I missiles and rockets stored in open areas are vulnerable to theft. The CDR should consider placing CAT I missiles and rockets in either an approved container (MILVAN, SEAVAN, or CONEX), or in a totally enclosed storage building. The following PSMs apply if a container or building is used:

(a) Doors will be secured with two approved field service padlocks.

(b) Access or possession of both building keys by one person is strictly prohibited.

(c) A key control system will be established so that no one person will be allowed to have access to keys for installed A and B locks.

(11) Commanders who routinely deploy for field training and live firing should consider having the support engineer activity construct a storage building to be used at the FLMSA. The building is not required to meet the minimum construction standards

for CAT 1 storage buildings in this regulation (earth covered), but should provide a degree of security necessary to enforce two person access and provide shelter from the weather. Type 2 outdoor magazines may be used as a temporary storage structure.

(12) When more than one unit uses the same area, stocks will be separated and identified by unit. One unit will be responsible for the security and access control of the entire area.

10-5. Portable Armories. Portable or deployable armories are authorized for the storage of CAT II through IV arms provided they are built to US Government specifications (Naval Surface Warfare Center (NSWC) 3046–93.2). Each portable armory will have a current DA Form 4604 that includes the serial number of the armory vault.

10-6. Operational Unit Ammunition (Non-training)

a. All arms rooms require a current Ammunition Storage License to store limited amounts of operational guard ammunition (5.56mm ball, 9mm ball, or .45 caliber for arming guards in the event of IDS alarm failure). The quantity of ammunition stored will be based on operational necessity not to exceed 100 pounds of net powder weight IAW DA Pam 385-64. NOTE: Any stored POW ammunition will also count towards the total allowable limit.

b. Commanders will authorize the storage of operational ammunition in writing.

c. Operational ammunition (non-training) will be requested by the unit's ammunition or supply section.

d. Ammunition will be hand receipted to the armorer on DA Form 5515, Training Ammunition Control Document, or DA Form 3161, Request for Issue or Turn-in, and/or DA Form 2062, Hand Receipt/ Annex Number, and on the armorers' hand receipt by Department of Defense Identification Code (DODIC), lot number, type, and quantity.

e. Ammunition will be accounted for and recorded on DA Form 2062 by type and quantity.

f. Operational ammunition (not training) will be permanently placed on the unit's PBO sensitive item hand receipt by Department of Defense Identification Code (DODIC), lot number, caliber, and quantity.

g. Magazines loaded with operational ammunition will contain a red diagonal stripe. At no time will loaded magazines be inserted in weapons when stored inside an arms room.

h. For Ammunition Storage license contact Post Safety Office at 624-3381/4303.

10-7. Secure Holding Area and Safe Haven

a. IAW AR 190-11, DODI/M 5100.76 DoD installations must accept AA&E shipments for safe haven or secure hold regardless of arrival time or final destination. Protection of shipment will be commensurate with the sensitivity of the AA&E. Under safe haven conditions or secure hold, explosive safety quantity distance requirements must be considered, but these requirements will not eliminate the responsibility to provide safe haven or secure hold to mitigate shipment vulnerability.

b. Granting a holding area does not relieve the carrier of liability and it is within the prerogative of the installation commander or activity representative as to whether carrier personnel are to remain with the shipment to fulfill security requirements.

c. IAW DTR 4500.9 Chap 205 DoD installations are required to assist commercial TSPs transporting DoD shipments of AA&E, classified (SECRET/CONFIDENTIAL/NWRM) sensitive, protected, HAZMAT, and CCI materials/shipments by providing secure holding and safe haven areas in the interest of public safety and national security. The installation or activity TFG page should articulate these requirements.

d. When considering TSP requests for assistance, installation CDRs and contractor facility directors shall take into account the current FPCON and the security requirements therein, as well as any Quantity Distance (QD) safety requirements, depending upon the commodity and Net Explosives Weight (NEW) of any explosives involved.

e. If the impacted vehicle contains SRC I or II AA&E, a secure holding area with Intrusion Detection System (IDS) or Closed Circuit Television (CCTV) shall be required if the driver leaves the load. The driver will only be given permission to leave in extreme national emergencies or severe life/limb or death medical emergencies. Normally, such a shipment will have two drivers and the second driver will assume responsibility for the shipment. If there is no second driver, the first driver has been released with the installation commander’s authority and no such area is available, the installation CDR/facility director shall make arrangements to post a 24-hour guard in lieu of the IDS or CCTV.

f. To provide secure holding of SRC I and II AA&E and SECRET material, the area shall be under Constant Surveillance (CS). CS can be met in either of three ways: (1) the area can be equipped with IDS and CCTV. (2) A security guard can be posted to provide dedicated continuous watch over the shipment—the security guard shall remain within 25 feet of the shipment, while maintaining full unobstructed view thereof. (3) Subject to the Commanding Officer/Officer in Charge (OIC) as reflected in local directives, driver(s) or other qualified carrier personnel can remain in the cab of the vehicle, if he/she is fully attentive to the task at hand (not in sleeper), or remains within 25 feet of the vehicle while maintaining a fully unobstructed view thereof.

g. Secure Hold Lot Area for Motor Vehicles Transporting Ammunition, Explosives, and SECRET material. An area of the installation or activity designated for the

temporary parking of commercial TSPs' motor vehicles transporting DoD-owned AA&E and SECRET material. Secure hold locations should be used for pre-planned, non-emergent stops.

h. Safe Haven. Safe haven is the act of permitting a motor carrier engaged in the act of transporting DoD AA&E or other sensitive items to park an impacted motor vehicle in a designated parking area on a DoD activity in response to an emergency situation. Emergency conditions may include civil disturbances, natural disasters, mishaps, vehicle breakdowns, terrorist activity, driver illness, or other emergent contingencies. Under these conditions, the DoD installation/activity in closest proximity to the scene of the emergency shall permit the motor vehicle to gain expedited access to the designated area on the installation for temporary parking. In the event the explosives contained on the vehicle(s) exceeds the NEW limits of the installation's secure holding area, or if the nearest DoD installation does not have a sited secure holding area, the installation/activity shall afford temporary parking on the installation/activity in accordance with DoDI 5100.76, and Service Policy (e.g. AR 190-11, AFI 31-101, and OPNAVINST 5530.13C).

10-8. Installation Responsibilities for Secure Holding Area and Safe Haven

a. Director of Emergency Services (DES) will accept all shipments of AA&E that arrive at ACPs, verify bill of lading and ID/Vet the driver(s), after duty hours will provide law enforcement escort shipment to secure holding area via approved ammunition route, ensure driver(s) are briefed to remain with the load, log all shipments and drivers names in DES MP journal and train all new DACP/DASG and annually thereafter.

b. Logistics Readiness Command (LRC) will ensure a current delivery schedule of all known after duty hours shipments is forwarded to DES on a weekly and as needed basis. Further, as the ammunition experts, select the primary and alternate locations for secure holding area and in coordination with safety ensure these areas meet requirements of DESR 6055.09 and all safety and ammunition regulations, references, updates and guidance's. LRC will be required to maintain and upkeep the secure hold area, to include any fence maintenance required.

c. Safety office in coordination with the LRC, Ammo Supply Point, QASAS will select and ensure the secure holding areas for explosives meet the requirements of DESR 6055.09, Edition 1 and all safety regulations, references, updates and guidance's.

d. Director of Plans, Training, Management and Systems (DPTMS) will establish a tasking system to provide an armed guard in the event the installation commander assumes responsibility for shipment in an emergency and write policy for all FPCON levels.

e. Transportation Officer (TO) will review (With IPSO) and upload Garrison Policy semi-annually into the Transportation Facilities Guide (TFG). Further, the TO will

maintain the correct points of contacts in the TFG system. TO will ensure a current delivery schedule of all known after duty hours shipments is forwarded to DES on a weekly and as needed basis.

Chapter 11
Security of Government Property

11-1. Government Computers. Marking of computers for ID purposes is done at the CDR's/DIR's discretion refer to AR 190-51, Appendix C. Recommend engraving wherever possible.

a. All doors and windows of offices containing government computers, office machines and their components will be secured when building is left unattended. Cable systems are highly encouraged.

b. Computer cable locking devices with keys will be listed on the DA Form 5513 and accounted for IAW AR 190-51, Appendix D.

c. Computers will be sub-hand receipted to the user level.

11-2. Specialized Security Equipment (Refer to AR 380-5). Government Service Administration (GSA) approved field safes and special purpose, one and two drawer, light-weight, security containers will be used for storage of classified information. Containers will be securely fastened to the structure or under sufficient surveillance to prevent their theft or compromise.

a. Government Service Administration map and plan files are available for storage of odd-sized items (e.g., computer media, maps, charts, and classified equipment).

b. Government Service Administration approved modular vaults, meeting Federal Specification AA–V–2737, may be used to store classified information as an alternative to vault requirements. For guidance in storing classified material refer to AR 380-5.

11-3. Supply Rooms and Equipment Storage Areas

a. Commanders/DIRs/FMs will designate a secure location for supply rooms and equipment storage areas. Caging material is authorized as long as walls extend to the true ceiling and is completely enclosed in a secure building.

b. Supply rooms will meet minimum structure security requirements per AR 190-51, Appendix B-2, or caging requirements of 3-28.

c. "Off Limits to Unauthorized Personnel" signs will be posted by entrance doors of supply rooms and equipment storage areas.

d. Access rosters will be posted by main entrances.

e. Keys and locks will be DoD approved and controlled IAW Army Regulation (AR) 190-51, Appendix D and this regulation.

f. See AR 190-51 for securing bolt cutters and other forced entry tools.

11-4. Army Property (Sensitive/Pilferage like items, Night Vision Devices (NVDs), Optics, Nuclear, Biological and Chemical (NBC), etc.)

a. Military property and equipment that is considered SIs, vulnerable to theft or portable equipment, (e.g., NVDs, tactical radios; lasers; combat optics; Interceptor Body Armor (IBA) vest/plates; bayonets, etc.) will be secured behind double barrier protection. EXCEPTIONS include:

(1) All AA&E items will be protected IAW AR 190-11.

(2) Any property with a security Controlled Inventory Item Code (CIIC) will be protected IAW AR 710-2 and this regulation.

b. Double barrier protection see AR 190-51, 3-12.

11-5. Secure Storage Rooms

a. A room must meet construction standards IAW AR 190-51, Appendix B to be considered a secure area.

b. Rooms used to secure high value items will have access control and display "Off Limits to Unauthorized Personnel" signs at entrance door(s).

c. Standard Form 701s will be used at the end of each duty day and maintained for a minimum of 90 days.

Chapter 12
Controlled Medical Items (Notes R, Q, C)

12-1. ICIDS Requirements

a. Ensure any facility utilizing ICIDS has an SOP for activation, deactivation, monthly testing and maintaining ICIDS logs.

b. Ensure ICIDS alarms signs are posted appropriately and where ICIDS is installed, there are at least two types of sensors being used.

c. Ensure duress switches installed at pharmacy dispensing windows and available for on-duty personnel at all times. Test all ICIDS alarms monthly, to include duress.

12-2. Security of Controlled Substances and Medical Resources

a. Security checks of isolated facilities will occur every 4 hours if not utilizing ICIDS, and facilities within hospitals not occupied will be checked at random intervals not to exceed 4 hours if not utilizing ICIDS.

b. Commanders must established written measures to safeguard controlled medical substance facilities at all times and report actual or suspected loss of controlled medical substances to Law Enforcement.

c. Pharmacies and Point of Use.

(1) Designate pharmacies with controlled medical substances restricted areas and ensure Pharmacies with controlled medical substances are constructed in accordance with AR 190-51, App B-2 (Secure Storage Structure).

(2) Ensure containers that contain Note R & Q items are locked when not in use and pharmacies have interior and exterior lighting sufficient enough to allow visual surveillance by security personnel.

(3) Pharmacy entrance doors (Restricted Area), will be locked at all times except when authorized personnel are entering or exiting.

(4) When authorized personnel are present, ensure Note R (Sch 2) substances stored in a double locked container, point-of-use machine, or automated dispensing system. When authorized personnel are not present, ensure Note R substances stored in approved point-of-use container or GSA Class V container.

(5) Ensure Note Q (Sch 3-5) substances are stored in an approved point-of-use container or if IDS available, in a container constructed of 20 gauge steel with a GSA approved locking device.

(6) Ensure end of day security checks are conducted by designated departing personnel on all controlled medical substance facilities and containers and annotated on SF 701 and SF 702.

(7) Ensure ambulances that store controlled medical substances are locked and checked every 4 hours when not in use and the items are secured in a commercially available storage container having user unique pin or biometrics, and the ability to create an automated audit trail.

d. Security of other Medical Resources.

(1) Ensure storage areas that contain human organs, blood products, radioactive materials, and surgical suites/oral surgery laboratories are secured when authorized personnel are not present. Also, access will be controlled, exterior lighting installed and signs posted with "Off Limits to Unauthorized Personnel."

(2) Ensure exterior openings such as windows less than 18 feet from the ground are covered with mesh or heavy gauge screens or equivalent materials in storage areas containing human organs, blood products, and surgical suites/oral surgery laboratories.

(3) Ensure storage areas containing high value items or highly pilferable items are constructed in accordance with the construction requirements in AR 190-51, App B-2.

(4) Ensure precious metals in any form are secured in a GSA approved class V container and surgical instruments, when not in use, are secured in a locked container and inventoried monthly.

(5) Ensure point of use or automated dispensing systems are locked when not in use and have posted signs stating "Off limits to Unauthorized Personnel," and exterior lighting installed.

12-3. Inventories. Monthly inventories of Note R, Q, and C controlled items will be conducted by a disinterested officer (E-7 or above, or GS-7 or above) and recorded on DA Form 1296, Stock Accounting Record Inventory. The same person cannot conduct consecutive monthly inventories.

Chapter 13
Airfield Security

13-1. Airfield Management Responsibilities. Airfields will be designated as "Restricted Areas" IAW AR 190-13 and signs will be prominently posted at a distance not to exceed 100 feet apart on the perimeter fence line. Signs must be readable at 50 feet when approaching.

a. The Airfield CDR and manager will establish a current and executable Airfield Physical Security Plan written IAW AR 190-13, App C. A copy of the finalized plan will be forwarded to the IPSO and appropriate commands/levels on the airfield.

b. An airfield PSO will be appointed in writing and will maintain liaison with tenant units.

(1) Physical Security Officers, as directed by the Airfield CDR, must conduct assessments/inspections of tenant units to ensure compliance.

(2) Establish and strictly enforce access badge procedures IAW AR 190-13.

(3) Conduct risk analysis on respective areas to ensure security measures are met IAW DA PAM 190-51.

c. Key and Lock Custodians will be appointed in writing by the CDR. Key control access to gates and other locations by airfield management will be strictly controlled IAW AR 190-51, Appendix D.

d. Access Control. Access to buildings associated with aviation facilities, aircraft parking areas and support equipment storage areas will be controlled at all times. Entrances and exits can be controlled through manpower, procedural, mechanical or electronic means.

e. Airfield Management will establish a Terrorism Counteraction Contingency Plan which will address:

(1) Airfield hijackings.

(2) Bomb threats/explosions.

(3) Shootings.

(4) Suicide/aircraft attack.

(5) Any other threat identified by the Airfield CDR. Note: Focus is to have a Plan of Action/Contingency plan in the event of incidents occurring on the airfield.

f. Security checks of parked aircraft will be conducted IAW AR 190-51 and AR 190-13.

(1) Risk Level I: Requires security checks not to exceed every four hours for unattended aircraft.

(2) Risk Level II: Requires security checks at least once every hour by a roving guard.

(3) Risk Level III: Continuous surveillance of aircraft by guards are required. ICIDS may be installed to eliminate continuous surveillance need.

(4) Security checks and records will be maintained at unit level for a minimum of 90 days. SF 701s or SF 702s will be established on all appropriate facilities, buildings, hangars, gates and doors.

g. Privately owned vehicles are strictly prohibited from the flight line or other areas where aircraft are parked.

h. Badge control measures will be strictly enforced in areas designated as restricted areas.

i. Tenant CDRs must coordinate with the Airfield CDR/manager regarding security matters.

j. End of Day Checks will be established and SF 701 will be used to annotate all checks on airfield facilities, windows, doors and gates.

13-2. Aircraft Weapons Systems

a. Will be parked with-in a lighted aircraft parking area with IDS or continuous surveillance when an aircraft is not in use and has mounted weapons.

b. Remove and store mounted weapons on aircraft or components in a secure location (e.g., arms room, ASP, an area under continuous armed surveillance or any structure meeting the requirements for storage of CAT I or II AA&E IAW AR 190–11).

c. Aircraft weapons systems will be made inoperable by removing barrels or firing mechanisms whenever practicable.

d. Weapon systems that are impractical to dismount due to operational readiness or probability of damage will be made inoperable by removing essential component(s), (e.g. electrical power on 20mm and 30mm weapon systems). When electrical power is the only essential component removed from the weapons systems, ammunition for those weapons systems will not be stored on the aircraft. Risk Level II security measures will apply IAW AR 190–51.

e. Aircraft equipped with manufacturer-installed or approved modification work order ignition and other door-locking devices which are not in use will be secured.

Locking devices and ignition keys will be controlled and accounted for on DA Form 5513. Personal retention of aircraft keys is prohibited. Duplicate keys serving as operational keys at maintenance facilities are prohibited. Aircraft will be parked in close proximity to each other when not stored in hangars.

13-3. Identification of Personnel on Aircraft.

a. Screening of arriving and departing aircraft at U.S. Army airfields and heliports. Senior/garrison commanders will develop and implement access control requirements to screen arriving and departing aircraft. All aircraft, passengers, and cargo arriving at or departing from Army airfields or heliports will be screened per access control requirements that will address the following situations, at a minimum:

(1) U.S. Government aircraft, if directed by the senior/garrison commander.

(2) Civilian and foreign aircraft on approved Army aircraft landing authorization numbers or civil aircraft landing permit (see AR 95–2).

(3) Aircraft executing an emergency landing.

(4) Any aircraft not scheduled or authorized to land at an Army airfield or heliport.

13-3. Bi-lateral Storage Memorandum of Agreement (MOA). Units storing property (e.g., NVDS, aircraft keys, fuel cards, etc.) in the same room/location must sign a bi-lateral storage MOU. The bi-lateral MOU will be signed and approved by all participating unit CDRs/FM and will establish overall responsibility to a responsible officer, who will prescribe control and accountability procedures for consolidated property.

Chapter 14
Barracks Physical Security Plan/Crime Prevention

14-1. Responsibilities

a. All units/agencies assigned, attached or tenant to Fort Knox (BDE/DIR/SQDN/BN/CO Level CDRs/FM), will:

(1) Establish a Barracks Physical Security Plan (BPSP) and Crime Prevention Program (CPP) and monitor its effectiveness.

(2) Appoint in writing a Crime Prevention Officer (CPO): SFC, GS-7 or Officer at the BN level; SGT or GS-5 at the company or facility manager level. Unit PSO and CPO will work together to ensure BPSP and CPP assist the command.

(3) Establish the BPSP and Crime Prevention SOP IAW AR 190-13, App D and AR 190-51, App C, F. Ensure the following areas are addressed: control of bolt cutters, entry and visitor control, visitor policies, security of mixed gender sleeping and personal hygiene areas, key control, security of sleeping areas, security of personal property, marking of personal and government property, emergency actions plans and prohibited activities. This chapter, although not all inclusive, will, serve to develop a unit's CP SOP. Standard operating procedures will include responsibilities for Charge of Quarters (CQ) to:

(a) Conduct security checks a minimum of two times before and after midnight of unit areas, to include but not limited to; mail orderly room; dayrooms/equipment, billet rooms, equipment storage areas, parking lots, motor pools, etc. Security checks will be recorded in the Staff Duty journal and kept on file for 90 days. Staff Duty personnel will also be provided a current BPSP and CP SOP, updated telephonic notification/contact rosters for unit personnel as well as emergency services (e.g., Sexual Harassment Assault Response Prevention hotline, suicide prevention hotline, and higher headquarters Staff Duty, if applicable).

(b) Comply with fire and safety requirements.

(c) Secure all doors except the main entrance doors after duty hours and ensure exits provide required safety, but deny entry.

(d) Properly secure and record any property found unsecured in the Staff Duty Journal.

(e) Report all incidents or suspected incidents to the CoC and to the Installation Provost Marshal Office IAW AR 190-45.

(f) Immediately report observed criminal acts or suspicious activity to the Fort Knox MP Station and chain of command and document such reports on the Staff Duty journal.

(g) Ensure building doors and windows are adequately secured.

(h) Ensure SDO/SDNCO duty log books contain a current billeting roster of personnel with their assigned rooms.

(i) Control visitor access to unit and billeting areas. Commanders will develop rules for visitors in the CP SOP.

(j) Prohibit access to minor juveniles 17 years old and younger, who are not US Military personnel, unless accompanied by parent or legal guardian.

(k) Deny access to personnel who have been identified by the CoC as prohibited entry into the billets.

(l) Prohibit vendors and solicitors access without prior written approval by the CoC.

(m) Crime Prevention Officers must conduct announced, unannounced and quarterly CP inspections and assessments of headquarters and subordinate CP programs. Crime Prevention Officers must maintain results via memorandum on file for 12 months.

(n) Crime Prevention Officers must ensure newly assigned personnel receive and acknowledge the unit CP in-brief within 10 working days of arrival to the unit. Crime Prevention Officers and first line supervisors will maintain a copy of their Soldier's CP Briefing in their personnel file.

(o) Crime Prevention Officers must schedule and conduct semi-annual CP training. Files will be maintained for 12 months.

(p) Crime Prevention Officer must comply with current AR directives and this regulation regarding structural, storage, and control requirements for safes, containers, locks, key control, etc.

(q) Crime Prevention Officers must ensure secure storage areas are available to store a Soldier's personal property and Organization Clothing and Individual Equipment (OCIE).

(r) Crime Prevention Officers must ensure Soldiers with high value dollar items ($100.00 or more) are inventoried and verified by a witness’s signature on High Dollar Value Sheets (HDVS), Personal Property Record when inventorying or declining to inventory their property. Completed and signed HDVS will be maintained and updated regularly by the CPO and the Soldier's First Sergeant. The Soldier's copy must be secured in an inconspicuous area at all times.

(s) Commanders and FMs must develop policies and procedures for the physical security of barrack rooms during periods of field training and short term deployments (e.g., NTC, JRTC, not to exceed 45 days).

b. Soldiers will:

(1) Secure private and government property at all times.

(2) Be encouraged to report suspicious activity or observed criminal acts to their CDR.

(3) Ensure assigned wall and foot lockers are in serviceable condition.

(4) Request through unit supply a new combination or replacement lock key if a combination is compromised or lock key is lost.

(5) Ensure government issued locks are not used to secure personal property.

(6) Encouraged to mark all personal property.

(7) Mark government property at direction of commander and IAW AR 190-51, App C.

(8) Not leave valuables and money in pillows, mattresses, or in unsecured night stands, desks, or lockers.

(9) MTOE/OCIE will not be stored in Privately Owned Vehicles (POVs) or military vehicles, on or off post for any reason. Commanders will ensure adequate and secure temporary storage is provided for those required to leave items unattended for inspections, training, etc. Items consisting in whole or part of AA&E are only authorized to be transported in government vehicles. Those failing to comply are subject to action under the Uniform Code of Military Justice (UCMJ), or other appropriate administrative action.

(10) Maintain OCIE.

(a) Issued clothing will be marked IAW AR 700-84.

(b) Individual clothing and equipment of Active Duty, Reserve and National Guard personnel living in troop billets will be secured by use of a locked wall locker, foot locker, duffel bag, or locked in a separate room. In lieu of a separate room, access to wall lockers may be controlled by modifying the lockers to accept a locking bar or by adding a second hasp and securing the locker with a second lock.

c. Unit Supply will:

(1) Establish security control measures for the security and issuance of bolt cutters AR 190-51, App F. Bolt cutters will be issued using a DA Form 5513 to establish

a chain of custody. All requests for bolt cutter issue will be approved by the unit First Sergeant.

(2) Ensure high dollar items have double barrier protection, (e.g., locked wall lockers inside a locked supply room).

(3) Provide a secure storage facility for personal property belonging to personnel on leave, TDY, hospitalized, deployed, Absent Without Leave (AWOL), or participating in field training exercises.

(4) Permanently mark commercial/military pilferage/high dollar items as directed by the CDR IAW AR 190-51, App C. Markings should not deface or devalue the item being marked.

(5) Supply storage rooms will be designated as “Off Limits to Unauthorized Personnel.”

(6) Post access rosters.

(7) Ensure electrostatic engravers or other methods are made available to Soldiers for marking personal property. Note: ID markings should be engraved wherever possible.

14-2. Dayroom/Barracks

a. Installation Off Limits Establishments/Off Limit Area signs will be posted on all unit bulletin boards.

b. Signs warning visitors to report to the SDO/CQ will be posted on all exterior doors to the billets or in areas where visitors will see the signs.

c. Visitor sign-in logs will be used and maintained by Staff Duty/CQ for a minimum of 90 days.

d. Visitor policies will be posted on all unit bulletin boards.

e. All rooms will be adequately secured when individuals are asleep or not present.

f. Dayroom televisions/DVD players and other high dollar government property will be sub-hand receipted to the Barracks or Supply NCOs. The property will be properly secured to stands or fixed objects and inventoried daily by the Staff Duty and monthly by a command appointed representative for proper accountability. IPSO recommends cable locks be used when appropriate.

g. Privately owned weapons are prohibited in the barracks.

14-3. Light Control Measures

a. Leave lights on in designated areas to reduce the potential for crime. These areas should include, but are not limited to, building exteriors, vehicle parking areas, troop paths, sidewalks, outside areas where troops congregate and those areas declared "OFF LIMITS."

b. A Staff Duty journal must be made and the CoC must be informed of all in-operative or inadequate lighting.

14-4. Security During Deployments

a. Commanders and supervisors are required to conduct recorded inventories of all stay behind equipment (SBE). An inventory of all barracks Soldiers' stay behind property (SBP) will be secured in approved containers, wall lockers or other secure locations. A security protective seal and padlock will be used to secure storage containers. Protective seal log procedures must comply with AR 190-51, Appendix D.

b. Commanders will establish unit SOPs to secure and provide access control to designated storage areas during deployment for POVs, all-terrain vehicles, boats, recreation vehicles, etc. Designated POV storage areas will be fenced and adequately lighted.

Chapter 15
Installation Access Control Procedures

15-1. Policy. Security personnel will verify the ID of all persons entering Fort Knox through the installation's visitor centers and vehicle access control points (ACPs) IAW AR 190-13.

15-2. Procedures

a. Screening and Vetting.

(1) Screening (Identity Proofing). Security personnel performing installation access control at the Visitor Control Center (VCC) will verify a person's need to have access to the installation and perform a visual inspection on all identification documents provided by visitors. When Automated Installation Entry (AIE) is not operational a physical (touch) examination will be conducted of all Identification cards. The inspection will include:

(a) Visual match of the photograph on the card to the person presenting the identification (ID) through the use of the authoritative database system known as AIE.

(b) Verifying authenticity by checking the anti-counterfeit or fraud protection embedded in the credential.

(c) Authenticating cards using AIE as the primary credentials for access.

(2) Vetting. Non-affiliated visitors requesting access will be checked against the Fort Knox Installation Bar List and the National Crime Information Center (NCIC) Interstate Identification Index (III). Those with a valid need to access Fort Knox will be granted access for one year at a time.

(a) Unescorted Personnel. Senior Commanders will not grant unescorted installation access without the required identity proofing, vetting and fitness determinations for all personnel who do not possess a CAC, or other DoD identification. Access will not be granted without completing a favorable NCIC-III screening which is the Army minimum baseline background check for entrance onto Army installations for non-Common Access Card (CAC) holders and visitors.

(b) Escorted Personnel. Escorts are required to remain with the Non-DoD person for the duration of the visit. Escorts must be in possession of an authorized DoD ID card to escort. Contractors in possession of a Common Access Card are not authorized to escort personnel that have not been formally vetted. Personnel that have undergone a NCIC-III check which is unfavorable may submit a request to be escorted on the installation with the approval of the Installation Physical Security Office.

(c) Juveniles 17 and under are not required to show proof of ID as a passenger. Juveniles are not required to have a NCIC-III check conducted. Juveniles who are driving a Privately Owned Vehicle must present either a DoD ID Card, or a valid state driver's license and must have an AIE pass.

b. Credentialing.

(1) Individuals shall be issued a separate ID card for each population category for which they qualify. In instances where an individual has been issued more than one ID card (e.g., an individual that is eligible for an ID card as both a Reservist and as a DoD contractor employee), only the ID card that most accurately depicts the capacity in which the individual is affiliated with the DoD should be utilized at any given time.

(2) The visitor's state Driver's License (DL) or Real ID Compliant Identification will be used for identity proofing credential. Visitors will be granted access based on a legitimate need not to exceed one year.

(3) Certain categories of personnel may require badge/pass in addition to their ID. The VCC will issue a pass from an Army approved badge/ pass system, such as the AIE Pass which will contain the individual's personal data, sponsoring agency or individual, whether they have escorted or unescorted access, and an expiration date. Badge/Passes will be issued based on a legitimate need and will not exceed one year. AIE Badges will be requested through the Installation Physical Security Office, by submitting a Memorandum for Request with all required information signed by the government Sponsor. Knox Hills residents not in possession of a DOD credential may be approved for an AIE plastic pass by presenting their lease at the Visitor Center. Plastic passes will only be issued for up to a year not to exceed the expiration date of the lease.

(4) Valid state picture ID is required for vetting and Identity proofing. Any groups that do not recognize the issuance of state ID cards will not be granted access to the installation.

c. Sponsorship.

(1) Only affiliated DoD ID card holders will be able to sponsor. Contractors in possession of a Common Access Card are not authorized to sponsor personnel. Sponsors are not required to remain with the Non-DoD person for the duration of the visit. All sponsors are responsible for the conduct of their guests and will inform the VCC when the sponsored individual's need for access is no longer required.

(2) Personnel requesting access to the installation who require a sponsor will be vetted and approved for access as needed after completing and submitting DES Form 118 (S) to the VCC.

d. Military Vehicles

(1) Military vehicles of any size and type may enter through any open gate and must possess valid ID IAW this program. Military vehicles LMTV or larger must have a ground guide at Wilson Gate. Military vehicles LMTV or larger must use oversize vehicle lanes at Chaffee and Brandenburg gates, no ground guides are required. ID cards for the driver or TC must be validated for each vehicle.

(2) Military Convoys consisting of 50 vehicles or more will be required to enter through Brandenburg gate from 0600-1300. Requesting access through Brandenburg gate or Baker gate after hours must be coordinated in advance during duty hours with the Installation Physical Security Office. If access is required after operating hours, call the DES at (502) 624-2111/2112.

(3) Military organizations requiring access through Limited Use Access Gates will coordinate prior with the Installation Physical Security Office and submit a request no later than 14 days prior to arrival. Installation Range Division may provide Access through a limited use gate to units training, provided they have received approval from the Installation Physical Security Office. Range personnel will validate information on the request with those being granted access.

(4) Military vehicles and military convoys will use the oversized lanes to the far right (Lane 6) or the furthest right lane. All personnel must be in possession of a valid ID. All drivers or TC must present ID and may vouch for the personnel in their vehicles.

e. Commercial Delivery Vehicles.

(1) Drivers must possess a current bill of lading for the specific delivery containing an address on the installation.

(2) Drivers must possess a valid state issued DL or Commercial Driver's License (CDL), a state vehicle registration and proof of insurance.

(3) All delivery vehicles are subject to a vehicle inspection at any time while on the installation. All delivery drivers must be cleared through NCIC-III. Government sponsors may escort individuals while on the installation in lieu of vetting using NCIC-III.

(4) If the vehicle has a seal, the seal's serial number will be checked against the bill of lading to validate authenticity. If the seal is broken or the serial number does not match a 100% inspection of the vehicle will be conducted.

f. Moving Companies.

(1) Drivers must possess a current bill of lading for the specific delivery containing an address on the installation.

(2) Drivers must possess a valid state issued DL, state vehicle registration, and proof of insurance.

(3) All delivery vehicles are subject to a vehicle inspection and all occupants will be vetted IAW this program.

(4) All drivers and occupants must request access and be cleared through NCIC-III. Government sponsor may coordinate with VCC for prior vetting.

g. Tow Trucks.

(1) Drivers must possess a valid tow tag, tow truck certificate of registration, tow truck application, cab-card, valid DL, state vehicle registration, and proof of insurance.

(2) All tow trucks are subject to a vehicle inspection and all occupants will be vetted IAW this program.

h. Recovery and Repossessions.

(1) Creditors, or their agents, requesting access to recover property based on default of a contract or legal agreement are required to coordinate through the Provost Marshal Office/DES Desk Supervisor.

(2) The Police Desk will provide an escort and notify the Installation Staff Judge Advocate (SJA). The creditor or their agent must provide a copy of title, contract or legal agreement; present evidence that the debtor is in default of the contract or legal agreement; present evidence they are working for the creditor.

(3) All drivers are subject to be vetted by NCIC-III prior to entry. Government sponsor will coordinate with VCC for prior vetting. Government sponsors may escort individuals while on the installation in lieu of vetting using NCIC-III.

i. Taxi Companies, Transportation Buses.

(1) Taxi drivers must be cleared through NCIC-III.

(2) Drivers must possess a valid state issued DL, valid taxicab operator's license, state vehicle registration, and proof of insurance.

(3) Vehicles are subject to inspection before access is granted.

(4) Taxi drivers will not be granted access as a trusted traveler.

(5) Passengers must possess valid ID and be vetted IAW this program.

j. Food Delivery Vehicles and Vendors.

(1) Vendors and drivers must apply for access and be cleared through NCIC-III.

(2) Drivers must possess a valid state issued DL, state vehicle registration and proof of insurance.

(3) All vehicles are subject to inspection prior to being granted access.

(4) Deliveries must have an on-post destination.

k. Special Events.

(1) The DoD requires all installations conduct a vetting process to determine fitness and eligibility for access. There are two categories of Special Events for DoD CAC holders and Non-DoD ID card holders, Installation and Hosted events.

a. Installation special events may be authorized IAW AR 190-13, Chapter 8-6, when NCIC-III screening is impractical and regulatory requirements may not be met.

b. When Installation special events have been declared by the Senior Commander, a risk analysis will be accomplished to assist in the development of additional security measures to mitigate any increased risk i.e. isolating event traffic and parking to specific locations, transporting attendees to and from the event utilizing government transportation, and directing event traffic to specific Access Control Points where access control measures are conducted prior to attendance.

(2) Hosted special events are small functions on the installation (i.e. weddings, proms, promotion ceremonies, etc.). Hosted special events should use the online 5 Day Fast Pass by going to https://visit.gvt.us/?b=usa&i=knox&t=v (Microsoft Edge, Firefox, Google Chrome, and Safari browser recommended). Further instruction are outline in item ee of this policy. Otherwise, the non-DoD visitors will proceed to the VCC and be vetted through NCIC-III IAW this program.

i. Gold Star Family Program.

(1) NCIC-III check will be conducted prior to enrollment in the program. The Fort Knox Survivor Outreach Services (SOS) Coordinator will coordinate directly with the Physical Security Office / VCC for vetting through NCIC-III prior to approving the enrollment request in the Gold Star Family Program.

(2) Fort Knox will issue Gold Star Family Member ID with survivor on the top from the Automated Installation Entry (AIE) system that is valid for 3 years from

the date of application. AIE Access Cards issued from other installations will be accepted at Fort Knox.

m. Family Care Plans. Units must coordinate with the VCC to ensure that when a Family Care Plan is executed, the care giver is properly vetted prior to gaining access onto the installation.

n. Family Visitors. All individuals who live on post must coordinate with the VCC to ensure that their visitors are properly vetted prior to gaining access onto the installation.

o. Trusted Traveler Program (TTP). The trusted traveler program is currently not authorized on Fort Knox.

p. The following are recognized Identification Cards for Access to Fort Knox:

(1) DOD CAC. DD Form 2A (ACT) (Active Duty Military Identification Card), DD Form 2 (ACT) (Armed Forces of the United States-Geneva Conventions Identification Card (Active)), DD Form 2 (RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Reserve)), DD Form 2 (RET) (United States Uniformed Identification Card (Retired)), DD Form 2S (ACT) (Armed Forces of the United States-Geneva Conventions Identification Card (Active)), DD Form 2S (RES) (Armed Forces of the United States-Geneva Conventions Identification Card (Reserve)), DD Form 2S (RET) (United States Uniformed Identification Card (Retired)), DD Form 2S (RES RET) (United States Uniformed Identification Card (Reserve) (Retired)), DD Form 1173 (United States Uniformed Services Identification and Privilege Card), DD Form 1173-1 United States Uniformed Services Identification and Privilege Card (Guard and Reserve family member), DD Form 2765 Department of Defense/Uniformed Services Identification and Privilege Card. Veterans Health Identification Card (VHIC) and the DoD Civilian Retiree Identification Card.

(2) Valid State Driver's License or Valid State ID Card with picture.

(3) Valid Passport issued from any government agency, valid Permanent Resident Card or valid United States work Visa provided they are escorted by an ID card holder and processed through the installation VCC office.

q. Special Agent Credentials. Any special agent of the Army's Criminal Investigation Division (CID), the Department of Defense Inspector General's Office (DOD IG), the Federal Bureau of Investigation (FBI), Department of Homeland Security Immigration Customs Enforcement (ICE), US Mint Police, or the Office of Personnel Management (OPM) who presents a badge accompanied by credentials issued to that agent for the purpose of conducting official business will be granted access to the installation.

r. Process for Access of Lost Identification. Those individuals claiming to be Service Members, Authorized dependents, or DA Civilians who arrive at the ACP

and claim they are assigned to Fort Knox, yet have no authorized ID in their possession, will be put in contact with their unit/ supervisor/ sponsor or the Police Desk so that an escort may be made available for access. Those individuals that have a valid Driver's License but no military ID will provide it at the VCC to be vetted and then allowed access to the installation without an escort with a positive adjudication of the NCIC-III check. Those with valid DOD credentials not in their possession who fail vetting will be required to be sponsored by someone in possession of valid DOD credentials.

s. AWOL Soldiers. AWOL or deserter personnel reporting to an ACP turning themselves over to Military Control will be detained and notification will be made to the Police Desk for further action.

t. HAZMAT Deliveries. All ammunition and hazardous material laden vehicles will be directed to Brandenburg Gate during duty hours or Baker Gate for access for after hours. To coordinate for access during duty hours, contact the Installation Physical Security Office at 624-8471/4788/1713. If access is required after operating hours, call the Police Desk at (502) 624-2111.

u. Access for Media Vehicles. All Media personnel will be required to be vetted, issued a pass and escorted by Public Affairs Office (PAO) personnel prior to being granted access to the installation. Media personnel are defined as anyone in a Media Vehicle/ News Reporting Vehicle or anyone who is reporting on the news for any agency. If Media personnel arrive to an ACP prior to PAO arrival they will wait at the ACP or VCC until PAO arrives to clear them.

v. Access for Funerals. Post Chapel or Casualty Affairs will contact the Police Desk prior to a funeral procession entering post. All vehicles in a funeral procession will be allowed access without checking ID, as long as the procession is escorted by Fort Knox Law Enforcement.

w. Emergency Vehicles. All marked emergency vehicles (police, fire and EMS) with local government license plates will be treated as a government vehicle and granted access after a check of their official credentials. During Higher FPCONs Drivers may be required to be validated prior to access being granted.

x. Knox Hills (Fort Knox Privatized Housing).

(1) Knox Hills residents that are evicted will have their access Credentials revoked and Knox Hills will provide notification to the DES. This does not apply to DoD personnel residing in Knox Hills.

(2) Knox Hills will coordinate with the VCC to ensure all employees Have been cleared for access and vetted through NCIC-III. Employees are issued an AIE Access Card.

y. School Sponsored Activities/Programs.

(1) Department of Defense Education Activity (DoDEA) school supported events where local community students from other schools will be participating on post will be cleared for access. School bus drivers and school chaperones will be vetted prior to gaining access to the installation.

(2) Buses may be boarded by security personnel to ensure there are no signs of distress.

(3) School Administrative staff may be issued installation passes or Badges when FPCON is elevated and access requires a pass.

(4) School Administrative staff will coordinate with the VCC to ensure all employees have been cleared for access and vetted through NCIC-III.

(5) Foreign exchange programs will be coordinated with the Installation Physical Security Office for Access Control. Foreign exchange students will be issued an AIE pass with sponsorship.

z. Foreign National Visitors.

(1) This policy addresses non-government-to-government visits and is not intended to cover all requirements for official visitors as identified in AR 380-10. Garrison, tenant and mission partner organizations that host official foreign government representatives must follow procedures in accordance with AR 380-10, appendix I, Department of the Army International Visits Program. All visits that involve the exchange of classified or other official government information must be coordinated through Foreign Disclosure channels. The DPTMS Garrison Security Office is the point of contact for these types of visits and can be reached at (502) 624-7442.

(2) Foreign Visitors 10 years of age or older are required to be sponsored for access to the installation. Escort must have authorized ID listed in Para 5p above. Foreign Nationals will be required to be sponsored prior to entry and will be granted escorted or unescorted access as determined by the Physical Security Office / VCC.

(3) Foreign Nationals will be required to obtain a badge/pass through the VCC or may obtain a badge/pass for up to seven days at Chaffee gate when the VCC is closed. Passes may be granted for short and long term. Short term passes will be issued for 30 days in duration. Long term visitors may be sponsored up to six months and receive an AIE pass for Access (Au Pair, Foreign Coaches, etc).

aa. Very Important Persons (VIP). The Garrison Commander may designate certain local, State, and Government Officials as VIPs. Once the designation is made staff will coordinate with VCC and process the VIP IAW the provisions of this program and issue an annual pass/badge or enroll that person in AIE for access.

bb. Fitness Determinations. DES personnel will determine if the person requesting unescorted or escorted access presents a potential threat to the good order, discipline or health and safety of the installation and will conduct fitness determinations IAW Army regulation and local policy. Department of the Army Security Guard personnel performing the access control mission and conducting the NCIC-III checks will inform the Sergeant of the Guard (SOG), Shift Supervisor or Captain of the Guard of any individual that has any of the following derogatory information on the NCIC-III check:

(1) The NCIC-III contains criminal information about the individual that causes the Senior Commander to determine that the individual presents a potential threat to the good order, discipline, or health and safety on the installation.

(2) The installation is unable to verify the individual's claimed identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.

(3) The individual has a current arrest warrant in NCIC, regardless of the offense or violation.

(4) The individual is currently barred from entry or access to a Federal installation or facility.

(5) The individual has been convicted of crimes encompassing sexual assault, armed robbery, rape, child molestation, production or possession of child pornography, trafficking in humans, drug possession with intent to sell or drug distribution.

(6) The individual has a U.S. conviction of espionage, sabotage, treason, terrorism or murder.

(7) The individual is a registered sex offender.

(8) The individual has been convicted of a felony within the past 10 years, regardless of the offense or violation.

(9) The individual has been convicted of a felony firearms or explosives violation.

(10) The individual has engaged in acts or activities designed to overthrow the U.S. Government by force.

(11) The individual is identified in the Terrorist Screening Database (TSDB) as known to be or suspected of being a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity. Security personnel performing

installation access control will strictly follow the Federal Bureau of Investigation's published engagement protocols.

cc. Access Denial Waiver Packet and Process. In cases where an individual is denied access based on derogatory information obtained from an NCIC-III check, the following process will be followed if the individual requests a wavier:

(1) Verify denied access status with the VCC at (502) 624-7011/7019/7014.

(2) Individuals must provide a certified copy of complete criminal history, which must include all arrests and convictions.

(3) Individuals must obtain a letter of support from the Government sponsor. The letter must indicate that the sponsor requests that the individual be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits. If the employee is terminated, the sponsor must inform the VCC that unescorted access to the installation is no longer authorized.

(4) Complete an installation Access Control Denial Wavier Application packet and provide to the sponsor, who will be responsible for submitting the wavier application to the VCC (Packet consists of all required documentation). All offenses must be listed, along with an explanation why the conduct should not result in denial of access to the installation. Other factors the sponsor/applicant should address are:

(a) Nature and seriousness of the conduct.

(b) Circumstances (in specific) surrounding the conduct.

(c) Length of time elapsed since the conduct.

(d) Age of the individual at the time of the incident or conduct, and proof of efforts toward rehabilitation.

(5) Provide a current physical or email address to enable the VCC to transmit a copy of his/her determination on the waiver request.

(6) The Government sponsor will review the individual's packet for completeness and determine whether or not to endorse the request for a waiver.

(7) If the Government sponsor decides to endorse the waiver, he/she must provide a letter of recommendation for the individual that addresses the conduct that caused the denial and indicate why the conduct should not prohibit the individual from being granted unescorted access to the installation. The Government sponsor will submit the packet and letter to the VCC.

(8) The VCC will review the wavier application and the designated government official(s) will make a fitness determination recommendation.

(9) The delegated official will review the waiver application and render a determination that ensures proper protection of good order, discipline, health and safety on the installation.

(10) If the delegated official does not grant the waiver request the Garrison Commander or Senior Commander may then review the waiver application for a subsequent/final determination.

(11) The VCC will receive access determination and will then provide a copy of the determination to the sponsoring agent and to the individual.

(12) Individuals who have had a waiver request denied may request reconsideration from the Installation Commander one year after the date of the final decision. Individuals may request reconsideration earlier if they present significant information that was not available at the time of the original request or show that the basis for the original denial was overturned, rescinded or expired.

(13) Limited Access Authorization. The DES may authorize limited access to barred individuals for entry to the installation or authorize access to areas other than their place of duty when an extreme hardship or compelling circumstance where no significant risk to the installation is present. This will be done on a case-by-case basis. Requests must be sent to DES Records Supervisor, at (502) 624-1776.

dd. 5-Day Fast Pass:

(1) U.S. citizens without a military ID but who have a valid state driver's license/ID and wish to visit Fort Knox for only a short duration should consider a 5-day Fast Pass. Those without a military ID and who wish to regularly access Fort Knox should see "Requirements to access Fort Knox under normal conditions" tab for instructions on how to obtain up to a 1-year visitor pass.

(2) There is no requirement to go to the Visitor Center for the 5-day Fast Pass.

(3) Registrant's driver's license serves as the pass.

(4) Steps to obtain the 5-day Fast Pass.

(a) Visit https://visit.gvt.us/?b=usa&i=knox&t=v (Microsoft Edge, Firefox, Google Chrome, or Safari browser recommended).

(b) Complete all pre-registration requirements on the secure site, being sure to select "5-Day Fast Pass." This process takes less than two minutes.

(c) Applicants should receive an SMS (text message) within minutes (and no later than 24 hours later) with notification on whether the request for a 5-day Fast Pass is approved. If no SMS is received, call the Visitor Center at 502-624-7011/7019 to check status.

ee. VCC Kiosk.

(1) U.S. citizens without a military ID but who have a valid state driver's license/ID and wish to visit Fort Knox may utilize the kiosk in the VCC lobby to obtain a 1-year paper pass. The kiosk requires a valid state driver's license or ID card and a smart phone for use.

(2) The "5-day Fast Pass" can also be obtained physically at the kiosk with a valid state driver's license or ID card and a smart phone. The driver's license or IDcard is the credential that will be presented to the guard at the gate.

(3) Personnel who do not have their DOD credential in possession may utilize the kiosk and choose the option "Forgotten ID" to obtain a 1-day paper pass.

(4) All of the above must still meet the requirements for access to the installation described above and will still be vetted via NCIC-III.

(5) During elevated FPCON's the Kiosk and Fast Pass may be turned off. Contractors and visitors may be restricted from entering Fort Knox.

15-3. Limited Use Gates

a. IPSO is the approving authority for access through all limited use gate. All of the Fort Knox's Main ACPs can handle oversized and special delivery trucks. Therefore, approval to access the installation through a limited use gates is only given when conditions absolutely necessitate their use. Normally, approval will only be given for special occasions for tactical vehicles, construction equipment, HAZMAT, special events, range access, and emergency access.

(1) **313/251 Gate**: Located on the South boundary of the installation and if approved, can be used for initial entry and final exit to and from to the Southern range facilities. Unit commanders must coordinate the use through range control and submit a signed memorandum to IPSO with the following information: explanation why a main ACP should not be used, dates and times of initial entry and final exit, numbers and types of vehicles, identify any ammunition transported onto Fort Knox, and identify and provide cell phone number of a senior leader responsible for training and on location. Further, the memorandum must acknowledge that the gate will only be used upon initial entry, final exit and emergency mission conditions. After approval by IPSO, a senior leader representative must coordinate with physical security office to receive access via key card or CAC enabling and be present while all vehicles enter gate to verify all occupants of vehicles.

(2) **Baker Gate**: Located on the West boundary of the installation and if

approved, can be used for convoys, special deliveries and special event access. Prior coordination will be made with IPSO.

(3) **Mt Eden Gate**: Located on the North Boundary of the installation and if approved, can be used for entry to and from North and East range facilities. Approval for this gate must be accomplished through a written memorandum of agreement between garrison and the entity using the gate. The use of this gate will incur cost as it is above baseline services. Further, Roger Hollow staff and contractors must be on an approved roster, have either a key card issued or CAC enabled and make an appointment with physical security for access.

Chapter 16
Security of Privately Owned Weapons (POW)

16-1. Purpose

This chapter establishes the criteria for possession, registration, transportation, storage, and disposal of firearms on Fort Knox.

a. Privately owned weapons and ammunition must be controlled. The Senior Commander (SC) has clear authority and responsibility to regulate privately owned weapons, explosives, and ammunition on Fort Knox. Personnel who remove privately owned weapons from Fort Knox will comply with applicable federal, state, and local laws pertaining to ownership, possession, and registration.

b. The carrying of privately owned weapons and ammunition on Fort Knox is only authorized following the established procedures in this regulation. Signs will remain posted at Installation Access Control Points (IACP) stating this prohibition.

c. This regulation is not intended to prevent the carrying of weapons by an officer, agent, or employee of a state, federal agency, or a political subdivision thereof while in an on-duty status, who is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law.

d. This regulation applies to registration of firearms belonging to personnel living on the installation and registration of firearms by personnel who bring a firearm onto the installation for the purpose of engaging in authorized activities such as hunting, dog training, or marksmanship events.

e. Privately owned weapons stored in unit arms rooms must be inventoried in conjunction with and at the frequency of the inventory of military weapons.

f. This regulation is punitive in nature. All individuals are subject to judicial processing under the US Magistrate Court system. Violations of this regulation may result in an apprehension, prosecution in the United States Magistrate Court, revocation of Weapons Permit, and temporary confiscation of privately owned weapons.

(1) Military violators are subject to Uniform Code of Military Justice (UCMJ) action, US Magistrate Court system, or appropriate administrative action.

(2) Civilian violators are subject to debarment from post, US Magistrate Court system, referral to civilian authorities, or disciplinary and administrative action according to appropriate civilian personnel regulations.

(3) Weapons utilized, possessed, transported, or stored in violation of this regulation may be temporarily or permanently confiscated.

g. Under the Assimilative Crimes Act, 18 U.S.C. § 13, when a criminal offense has been committed on Fort Knox, and the offense is not a federal offense, Kentucky law

may apply to the offense. Any person found guilty of violating any state weapon offense, Fort Knox weapon rule, or regulation made applicable to Fort Knox under the provisions of this regulation may be subject to a fine and/or imprisonment, or both, for each violation per Public Buildings, Property, and Works (40 U.S.C. § 318c) and (40 U.S.C. § 1315 (c)(1).

16-2. Responsibilities

a. Unit Commanders:

(1) Account for and inventory privately owned firearms and ammunition secured in unit arms.

(2) Ensure that a DA Form 3749 (Equipment Receipt) has been issued for each privately owned firearm secured in the arms room. Privately owned firearms will be inventoried in conjunction with and at the frequency of the inventory of military weapons.

(3) Establish limits on the quantity and type of privately owned ammunition stored in the arms room, based upon availability of space and safety considerations.

(4) Ensure that inspections are conducted IAW with AR 190-11 and AR 190–13 and this regulation to ensure proper storage and control.

(5) Take possession of unauthorized weapons or unregistered firearms and coordinate with DES for registration and/or proper disposition.

(6) Post applicable local regulations and state and local law information on ownership, registration, and possession of firearms and ammunition on unit bulletin boards.

(7) Brief all newly assigned persons on this regulation and subordinate command guidance. All personnel will be made aware of changes.

(8) Ensure all POWs within their command whose owners reside on post, stored in company arms room, or are transported on post for authorized events are registered through DES. Verify proof of legal ownership of the firearm and that the individual is not prohibited from possessing a firearm IAW AR 190-11 and Federal law.

b. Directorate of Emergency Services (DES):

(1) Register privately owned firearms IAW AR 190-11 and issue weapons permits or denial to register/revocations firearm letters as appropriate.

(2) Verify firearm registration and proper firearm storage during IACP operations.

(3) Confiscate unlawful and unauthorized weapons during normal law enforcement operations and dispose of them IAW AR 190-11 and the DES Standing Operating Procedure (SOP).

(4) Conduct a Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE) trace on all firearms involved in criminal activity and an eTrace and NICS check prior to returning any firearm that was taken by Law Enforcement during an investigation ensuring no POW is released to a person who is prohibited.

(5) Enter lost, stolen or recovered firearms in the National Crime Information Center (NCIC) terminal.

(6) Upon receipt of Civilian Protective Orders (CPO) or Military Protective Orders, verify if any firearms are registered on Fort Knox. If yes, notify unit Commander and ensure firearms are surrendered and secured in unit arms room or turned-in to the county sheriff as directed in the (CPO).

(7) May approve Department of Army Civilian Police (DACP) to transport and store unloaded POWs to and from work in proper configuration and lockable container.

c. Directorate of Family Moral, Welfare and Recreation (DFMWR) -

(1) Verify the registration document of each person requesting to utilize facility prior to authorizing marksmanship activities utilizing a privately owned firearm.

(2) Direct owners of unregistered firearms to DES and instruct owners of unregistered firearms to remove the weapons from the installation until such time as the weapons are registered.

d. Directorate of Public Works (DPW) – Hunt Control:

(1) Verify the registration document of each person requesting to utilize a hunting area.

(2) Direct owners of unregistered firearms to DES and instruct owners of unregistered firearms to remove the weapons from the installation until such time as the weapons are registered.

e. Army and Air Force Exchange Service (AAFES): Inform firearm purchaser about the Fort Knox weapons registration requirement.

f. Individual possessing, storing, or transporting privately owned weapons and ammunition:

(1) Submit FK Form 2759-E (Registration of Privately-Owned Weapons) for any personnel requesting to bring firearms on Fort Knox.

(2) Must present proof of registration for National Firearms Act (NFA) firearms.

(3) Immediately report the permanent removal from post, loss or sale of registered privately owned weapons to the DES and unit chain of command.

(4) Immediately report the use of privately owned weapons for other than authorized hunting or marksmanship activities to the DES.

(5) Declare privately owned firearms to security guards when entering through an IACP.

(6) If approached by law enforcement or security personnel, immediately declare if weapons are on their person, in their residence, or in their vehicle. If requested by installation law enforcement personnel, individuals will present the registration document when the firearm is out of an approved storage location and being transported on the installation.

(7) Do not enable prohibited personnel (listed in paragraph 16-10) to possess, store, or transport firearms or dangerous weapons.

(8) Store weapons properly IAW AR 190-11 and this regulation

16-3. Prohibited privately owned weapons

a. Various statutes make possession of the following firearms or ammunitions unlawful:

(1) A stolen firearm (18 U.S.C. § 922(j)).

(2) A machine gun that was not possessed before May 19, 1986 (18 U.S.C. §922(o)).

(3) A firearm that is not detectable by metal detectors or x-ray machines (18 U.S.C. § 922(p)).

(4) A NFA weapon not registered to the person in the National Firearms Registration (26 U.S.C. § 5861(d)).

(5) A firearm with the serial number obliterated, removed, changed, or altered (26 U.S.C. § 5861(h)).

(6) A firearm without a serial number as outlined in 26 U.S.C. § 5861(i).

b. Any weapon of mass destruction.

c. Any explosive weapon.

d. Any hoax bomb - a device that reasonably appears to be an explosive or incendiary device; or by its design causes alarm or reaction of any type by an official of a public safety agency or a volunteer agency organized to deal with emergencies, except authorized military training aids.

e. Improvised firearm - a device or devices that were not originally a firearm and are adapted to expel a projectile through a smooth or rifled-bore barrel by using energy generated by an explosion or burning substance.

f. Armor-piercing ammunition.

g. NFA Firearms that are classified as: Any Other Weapon; Destructive Devices. EXCEPTION: Shotguns or shotgun shells with a bore over 0.50 of an inch for sporting purposes are authorized.

16-4. NFA firearms

a. Authorized types: Short barrel shotguns; Short barrel rifles; Machine guns and automatic weapons; Suppressors.

b. Carry: Prohibited on Fort Knox (to include school grounds and Federal Buildings) except for registered storage location and authorized hunting/sporting areas. Guidelines for transportation are outlined in Chapter 16-12 of this regulation.

c. Possess: The registered owner must be present. Contact Fort Knox Hunt Control at 502-624-7311 for authorized use on Fort Knox.

d. Storage: Must be secured so that no one other than the NFA registered person has access to them.

(1) Family housing. The service member's commander must authorize all NFA firearms stored in housing. Firearms must be stored in either a secured safe, locked container, gun rack, and recommended secured with an approved trigger or chamber style gun lock that prevents loading or firing. Ammunition will be secured in a locked container, separately from NFA firearms.

(2) Transient lodging. Individuals in transient lodging may not store firearms in IHG facilities as there is no approved storage.

(3) Geographical bachelor quarters. The service member's commander must authorize all NFA firearms stored in geographical bachelor quarters. Firearms must be stored in either a secured safe, locked container, gun rack, and recommended secured with an approved trigger or chamber style gun lock that prevents loading or firing. Ammunition will be secured in a locked container, separately from NFA firearms.

(4) Single Soldier barracks. Individuals living or staying in single Soldier barracks or unaccompanied personnel quarters must store NFA firearms and ammunition in the unit arms room.

e. Registration: Firearm must be registered with the National Firearm Registry. Firearm must be registered with DES, if brought onto Fort Knox.

16-5. Firearms other than NFA firearms

a. Authorized types: Handguns; Rifles; and Shotguns.

b. Carry: Prohibited on Fort Knox (to include school grounds and Federal Buildings) except for registered storage location and authorized hunting/sporting areas. Guidelines for transportation are outlined in Chapter 16-12 of this regulation.

c. Possess: A Fort Knox weapons permit holder not under the influence must be present. Contact Fort Knox Hunt Control at 502-624-7311 for authorized use on Fort Knox.

d. Storage: Must be secured in a container inaccessible to children and unauthorized individuals.

(1) Family housing. The service member's commander must authorize all firearms stored in housing. Firearms must be stored in either a secured safe, locked container, gun rack, and recommended secured with an approved trigger or chamber style gun lock that prevents loading or firing. Ammunition will be secured in a locked container, separately from NFA firearms.

(2) Transient lodging. Individuals in transient lodging may not store firearms in IHG facilities as there is no approved storage.

(3) Geographical bachelor quarters. The service member's commander must authorize all firearms stored in geographical bachelor quarters. Firearms must be stored in either a secured safe, locked container, gun rack, and recommended secured with an approved trigger or chamber style gun lock that prevents loading or firing. Ammunition will be secured in a locked container, separately from firearms.

(4) Single Soldier barracks. Individuals living or staying in single Soldier barracks, unaccompanied personnel quarters, or transient quarters must store firearms and ammunition in the unit arms room.

e. Registration: Must be registered with DES, if brought onto Fort Knox.

16-6. Dangerous or deadly weapons other than firearms

a. Authorized types: BB/Pellet gun; pepper spray; stun gun; Taser; potato gun; spear guns, long bows, compound bows, blowguns, other projectile launching devices, swords, knives, household instruments, such as utensil knives, and kung-fu weapons (crossbows, nun chucks, and throwing stars).

b. Carry: Prohibited on school grounds and federal buildings.

Note: Pocket knives with a blade less than 2 ½–inches in length and personal defense items, such as pepper spray, stun gun, and Taser, are permitted in federal buildings with facility managers approval, but not on school grounds.

c. Possess: An adult not under the influence must be present; parent permission and adult supervision is required for minors.

d. Storage: Must be secured and inaccessible to children and unauthorized individuals.

e. Registration: None.

16-7. Concealed privately owned weapons

a. The carrying of concealed privately owned weapons on Fort Knox is strictly prohibited, regardless of whether a state or county permit has been obtained. For the purpose of this regulation, a concealed weapon is any instrument used or designed for the purpose of inflicting grievous bodily harm that is carried on the person in such a way as to be hidden from ordinary view.

b. The senior commander is the approving authority for Law Enforcement Officers Safety Act (LEOSA) exceptions. Granted exceptions along with the Fort Knox Registration permit must be in possession when carrying the firearm on the installation.

16-8. Authorized hunting

a. Hunt control will provide weapons restrictions based on type of game being hunted and time of year.

b. Privately owned weapon possession is prohibited while under the influence of drugs or alcohol.

16-9. Federal buildings

a. Federal law prohibits the possession of firearms in federal facilities by all individuals not specifically authorized by 18 U.S.C. § 930. Violators will be subject to fine and/or imprisonment for periods up to five years.

b. All buildings on Fort Knox which provide customer service functions will display a sign, clearly posted at each public entrance, to serve notice required by 18 U.S.C. § 930a. The FK Label 190-11(Figure 3-1 Warning Label – Weapons Prohibited in Federal Buildings) may be used to identify the facility as restricted.

c. Commanders and building managers may post the notice for command and headquarter facilities, mission-essential facilities, and other selected facilities as appropriate.

d. Tenant organizations may further restrict what kind and type of personal defense weapons and utility items, such as multi-tools, are allowed into their respective buildings. These restrictions must be outlined in the organization’s physical security plan.

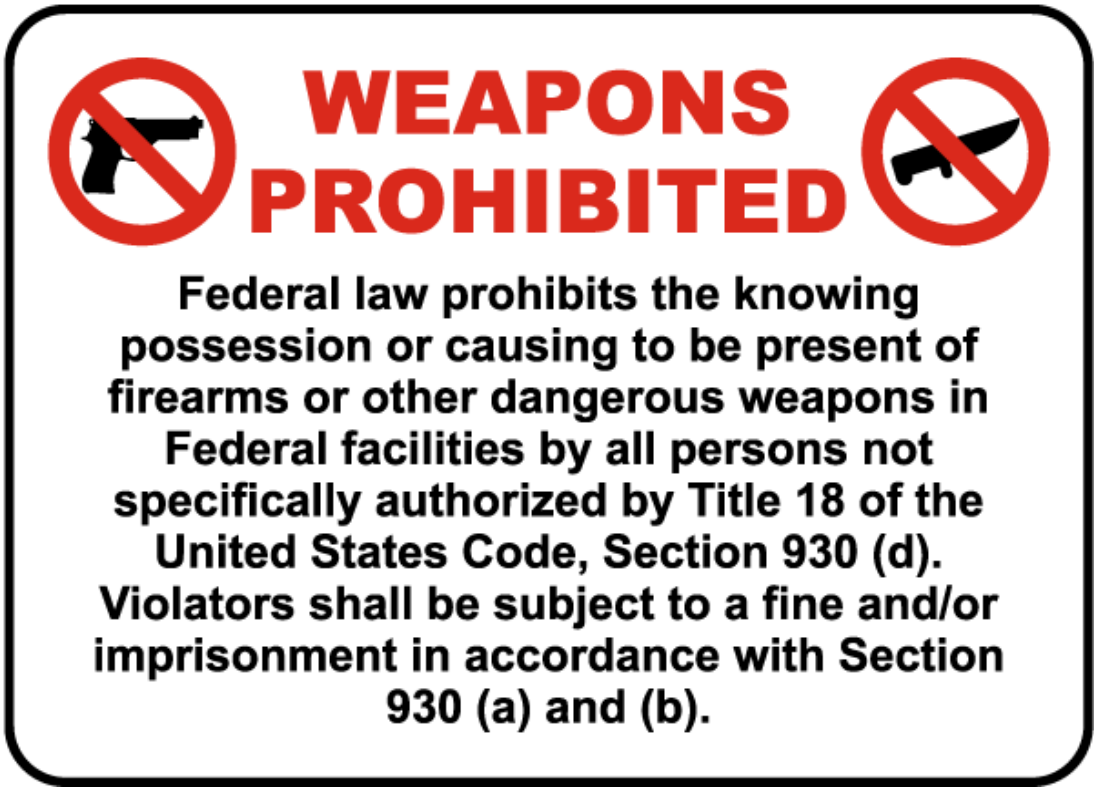


Figure 16-1

16-10. Individuals prohibited from possessing firearms

a. Title 18 U.S.C. § 922(g) establishes nine categories of individuals who may not possess firearms or ammunition. Title 18 U.S.C. § 922(d) makes it unlawful for any person to give any firearm or ammunition to a person, if he/she knows or has reasonable cause to believe the person is in one of the nine categories.

b. The categories are any person who–

(1) Has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year.

(2) Is a fugitive from justice.

(3) Is an unlawful user of or addicted to any controlled substance.

(4) Has been adjudicated as a mental defective or has been committed to a mental institution.

(5) Is an alien illegally or unlawfully in or admitted to the United States under a nonimmigrant visa.

(6) Has been discharged from the Armed Forces under dishonorable conditions.

(7) Having been a citizen of the United States, has renounced his or her citizenship.

(8) Is subject to a court order that restrains the person from harassing, stalking, or threatening an intimate partner or child of such intimate partner.

(9) Has been convicted of a misdemeanor crime of domestic violence.

c. All individuals under 18 years of age may only possess firearms when supervised by an adult with a Fort Knox weapons permit/registration in authorized locations during authorized marksmanship or hunting.

16-11. Individuals prohibited from registering firearms

a. There are six categories of individuals who may not register firearms IAW AR 190-11.

b. The categories are any person who–

(1) Has been convicted of a felony (Gun Control Act of 1968 (18 U.S.C. § 921 et seq.), as amended in 1996 (18 U.S.C. § 922)).

(2) Has been convicted in any court of a misdemeanor crime of domestic violence or a felony (the Lautenberg Amendment to the Federal Gun Control Act of 1968, as amended in 1996).

(3) Is a fugitive from justice.

(4) Has been convicted in any court of the possession, use, or sale of marijuana, dangerous or narcotic drugs (the term convicted includes non-judicial punishment under UCMJ, Article 15).

(5) Is presently declared as mentally incompetent or who is presently committed to any mental institution.

(6) Any Civilian or Family member under the age of 18 is prohibited from the use of firearms, unless accompanied and supervised by a parent or legal guardian over the age of 18.

16-12. Privately owned weapon transportation

a. Transporting of a loaded firearm in a vehicle is prohibited. Muzzle loading firearms will be considered as unloaded when the ignition system (cap or powder in pan) is removed.

b. Fort Knox uses the Automated Installation Entry (AIE) system and all Firearms must be declared to the Security Guard when entering through an IACP.

(1) Individuals bringing weapons onto Ft. Knox will by-pass the scanning pedestal and proceed directly to the guard in the booth and declare firearm(s).

(2) Individual must present their picture identification (ID) and their Fort Knox weapons permit/registration, directly to the guard.

(3) Individual must state purpose of bringing firearm onto Fort Knox (for example, storage, marksmanship, or hunting).

c. Individuals must travel in a direct route to and from the authorized area. While in transit between authorized areas, brief stops may be made at the Main Exchange, the Express(s), and the Hunt Control facilities. Weapons will not be removed from the vehicle during these stops. While transporting, weapons that fire a projectile by means of tension cables/bands, and/or springs (crossbows, spear guns, and bows) must be de-cocked and the projectile removed from the rail and/or nock point.

d. No other stops are authorized and firearms will not be stored in vehicles while at work.

e. Personnel removing firearms from Fort Knox will comply with applicable Federal and Kentucky laws pertaining to ownership, possession, and registration. Firearms must remain in the proper transport configuration until personnel are clear of the installation boundaries.

f. Individuals traversing Fort Knox from one off-post location to another off-post location using a publicly traveled roadway without stopping to conduct an activity within the confines of Fort Knox may transport weapons in accordance with Kentucky State Law and will not be held to the provisions of this regulation.

g. All firearms will be transported in the vehicle trunk for sedans or cased and stored not in plain view from outside the vehicle for SUVs and pick-ups. Firearms in a “gun sock” or holster will not be considered cased. A firearm enclosed in a standard hard or soft case is considered NOT in plain view. At no time should a firearm, cased or uncased, be transported in window gun racks. Under no circumstances may an uncased gun be transported under or behind a seat or in a glove compartment, console, seat pouch or similar location. Commercially available trigger locks and other security devices are strongly recommended to deter and to prevent loss or theft.

h. Ammunition may be stored in the same container as the firearm but must be unloaded from the firearm.

16-13. Privately owned weapon storage

a. Privately owned weapon(s) stored in unit arms storage facility will be provided the same protection afforded to military weapons and will be stored separately from military weapons. They will be inventoried at the same interval as military weapons.

b. Privately owned weapon(s) stored in on-post housing will be stored in a locked container or provided with a trigger lock. Ammunition for the firearm must be unloaded from the firearm but may be stored in the same locked container.

16-14. Registration requirement

a. All firearms brought onto the installation for storage or to engage in authorized activities must be registered through the DES.

b. All individuals 18 years of age and older in possession of a firearm must have the firearm registered in their name. A single firearm may be registered to more than one person.

c. Service members in the grade of O-5 and below must have their commander's approval; Service members in the grade of O-6 and above may sign for themselves.

d. Family members will follow the same procedures outlined in paragraph 4-1b.

e. Civilians and retirees sign for themselves.

16-15. Registering procedures

a. All individuals must complete FK Form 2759-E. This form is available on the Fort Knox Garrison website at http://www.knox.army.mil/Garrison/dhr/asd/forms.aspx. The form may be typed or hand written. At no time may the Fort Knox 2759-E form be modified. Valid state-issued identification card must be presented with the registration form. All newly assigned personnel or personnel already residing on Fort Knox who purchase or bring a new firearm onto Fort Knox have 24 hours to get firearms temporarily registered.

b. Temporary registration may be conducted for all newly assigned personnel on PCS orders or recently purchased firearms with receipt by bringing a completed FK Form 2759-E to VCC. After duty hours take the registration form to Chaffee Gate. These personnel will receive a seven day temporary permit that allows the firearm to be brought onto the installation for proper storage only as outlined in 16-4-6/13 of this regulation and allow full registration process to be completed. The temporary permit does not authorize the use of the firearm for any reason on the installation, such as hunting or marksmanship.

c. Firearms will be registered by dropping off a completed copy (signed by unit commander if applicable) of Fort Knox form 2759-E at the Fort Knox Visitor Control Center (VCC). Registrations will be completed and ready for pickup within seven (7) days.

d. Alternatively, FK Form 2759-E may be mailed to the DES, ATTN: Physical Security, 481 Gold Vault Rd, Bldg. 298, Fort Knox, KY 40121. If mailed, the form must be accompanied by a copy of the registrant's valid state-issued identification. If the registration form is mailed, accurate telephone numbers are critical so telephonic contact may be made to clarify any issues. Registrations will not be mailed back and must be picked up in person.

e. Do not bring firearms into any facility for registration.

f. Changes in registration information must be immediately provided to DES. Firearms registration will be valid for three years and should be un-registered when an individual no longer possesses the firearm.

g. Registration permits may be picked up at the Fort Knox Visitor Center during operational hours only. Sponsors may pick up forms for authorized dependents only.

16-16. Weapons permit/registration appeals/ revocations

Procedures must be explained in the permit denial letter. Individuals prohibited by law from possessing a firearm may not appeal.

a. Weapons registration denial.

(1) Personnel will have their registration denied when derogatory information is identified in the background check.

(2) It is the responsibility of the individual to obtain necessary documents that may clear the derogatory information and submit the documents to the VCC.

b. Those personnel found to be in violation of this regulation for transportation, storage and/or declaration will have their privileges revoked for a period of one year. Weapons registration will be confiscated or turned in to the VCC within 24 hours for all personnel that have their privileges revoked on the installation.

c. After one year those individuals may request to register their firearms on the installations.

d. Individuals eligible for an appeal may submit formal written appeals through the DES.

e. Service members and Family members require recommendations from the Service member's unit commander for appeals.

f. All appeals require recommendations from the DES and Staff Judge Advocate (SJA).

g. The Garrison Commander (GC) is the appellate authority for appeals denied by the DES.

h. The SC is the final appellate authority for appeals denied by the GC.

16-17. Exemptions

The following personnel, entities, groups, and weapons are exempt from all or parts of this regulation.

a. Small arms and ammunition issued to general officers are exempt from all provisions of this regulation, except loss and investigations requirements.

b. Organizational weapons (for example, Boy Scouts, 4-H, Meade County Sportsman Club, etcetera) are exempt from registration, but are still required to comply with transportation requirements. Organizational weapons are not owned by any one person, but are owned by the organization collectively and procured with organizational funding. Organizations must make prior coordination with DES to bring weapons on the installation for special events.

c. Muzzleloader/black powder firearms, antique firearms, and firearms manufactured prior to 1968 bearing no serial number are exempt from registration; however, they are still required to comply with transportation and storage requirements.

d. Weapons identified in paragraph 16-6 and any other weapons that fire a projectile by means of compressed air are exempt from all portions of this regulation. Weapons that fire a projectile by using tension cables/bands, and/or springs are NOT exempt from this regulation, but do not have to be registered.

e. Individuals who do not enter Fort Knox through an IACP and traverse on or through Fort Knox jurisdictional areas on public roadways: 31W, 60, 313, 1500,1638, or 1816 that do not stop to conduct any activity are exempt from all portions of this regulation. (NOTE: Fort Knox jurisdiction begins approximately 9 nine feet off of these roadways.)

f. Individuals of a government carrier service with a government bill of lading requiring armed guard surveillance are exempt from registration, but must comply with all other portions of this regulation.

g. Any officer, agent, or employee of a federal agency, a state, or a political subdivision thereof while in an on-duty status, who is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of law is exempt from registration and storage but must comply with all other portions of this regulation.

16-18. Federal Firearms License (FFL) and Operating a Firearms Business on Fort Knox

Senior Commander has strictly prohibited the operating a private firearms business on Fort Knox (except AAFES). This includes but not limited to selling, repairing and manufacturing firearms as defined by ATFE for profit of any manner. Operating a Firearms business is defined by ATFE guidance. Courts have identified several factors relevant to determining on which side of that line your activities may fall, including: whether you represent yourself as a dealer in firearms; whether you are repetitively buying and selling firearms; the circumstances under which you are selling firearms; and whether you are looking to make a profit. Note that while quantity and frequency of sales are relevant indicators, courts have upheld convictions for dealing without a license when as few as two firearms were sold, or when only one or two transactions

took place, when other factors were also present. If you are unsure contact the local ATFE office.

Chapter 17
Civilian Small Unmanned Aircraft Systems (UAS) and Drones

17-1. Purpose.

This chapter establishes the Fort Knox policy the management and use of non-official unmanned aircraft systems (UAS) on Army installations. An unmanned aircraft (UA) is defined as an aircraft operated without the possibility of direct human intervention from within, or on, the aircraft. An UAS is defined as a UA with associated elements, to include communication links and components that control the UA. UAS include remote controlled aircraft capable of sustained flight in the atmosphere, including multirotor, drones, helicopters, fixed-wing aircraft, and other model aircraft.

17-2. Background.

Background. Public Law 112-95 defines unmanned aircraft as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. Section 336 of P.L. 112-95 defines a model aircraft as an unmanned aircraft that is capable of sustained flight in the atmosphere, flown within visual line of sight of the person operating the aircraft, and flown only for hobby or recreational purposes. Unmanned aircraft, including RC model aircraft, may pose a hazard to manned aircraft in flight and to persons and property on the surface if not operated safely. RC model aircraft operations that endanger the safety of the National Airspace System (NAS), particularly careless or reckless operations or those that interfere with or fail to give way to any manned aircraft, may be subject to FAA enforcement action. Increasing UAS activity on, or near, Army installations raises safety and security concerns. These include overflights of military installations, flight safety hazards to military aircraft, and possible illicit use by criminals and adversaries. Meanwhile, counter-UAS capabilities for base perimeter detection, ID, tracking, point defense, and defeat of UAS are still limited. These factors underscore the need for installation commanders to develop and implement guidelines for regulating Army personnel hobby and recreational UAS use on Army installations and for responding to suspicious UAS activity.

17-3. Responsibilities.

(a) The Federal Aviation Agency (FAA) provides policy for regulating the flight of UAS in the U.S. air space to include UAS flight over Army property. By request of the DOD, the FAA has established UAS-specific flight restrictions over specific DOD installations and sites which are particularly national-security sensitive and vulnerable to potential UAS-based threats. These UAS-specific flight restrictions are known formally as special security instructions (SSI). Though the initial number of Army installations protected by SSI is very small, the FAA and the Army will implement SSI for more qualifying Army locations in the future.

(b) Director DPTMS will establish and maintain an installation policy letter in conjunction with Godman Army Air Field (GAAF). Further, GAAF Air Operations will be responsible for reporting any violation of GAAF or Fort Knox to the FAA, during normal tower operations.

(c) Director DES, will ensure law enforcement responds to all reports of UAS operating in and around Fort Knox and GAAF. Establish and maintain DES policy directing the following:

1. Respond to reports of unauthorized, suspicious, harassing, unsafe, or dangerous use of UAS.

2. If applicable, immediately notify the Air Traffic Control Tower.

3. If the UAS poses a physical threat to personnel or resources, respond with measures consistent with the standing rules for the use of force (SRUF).

4. Notify local LE in accordance with the procedures previously established with local LE officials.

5. Notify installation authorities, operations center, duty staff, and/or Criminal Investigative Division.

6. Execute appropriate police action: at a minimum, stop, identify, and interview the operator(s).

(a) Locate the operator. Direct attention outward and upward to attempt to locate individuals who are holding a controller or device that appears to be operating an UAS. Look at parked or moving vehicles, windows, balconies or roof tops.

(b) Interview operator and collect the following information:

(1) Name, address, and positive ID of operator.

(2) Ask UAS operator for the type of operation and to present appropriate documentation. The operator must provide the registration certificate (paper or electronic) upon request.

(3) Record registration number, and verify markings on the UAS.

(4). Detailed description of the UAS.

(5) Document time, place, and details of flight. Take pictures and interview witnesses, and so forth.

7. Report all incidents to and coordinate with GAAF, CID, FBI, and FAA investigators as appropriate. This includes, MP Desk will report and submit all suspicious UAS activity using the FBI's eGuardian system and contacting FAA Regional Operations Center during non-duty hours.

(d) PAO will conduct UAS awareness campaigns, including information about installation UAS regulations and policies, on the installation and in the local community. Highlighting unauthorized use of UAS from within an installation subjects the operator to possible punishment under either the UCMJ, or Federal or State law as well as potential forfeiture of any unauthorized recordings, photographs, or videos. Pursuant to 50 USC 797, violations of a defense installation property security regulation, or an installation UAS policy may be punished as a Federal criminal offense.

(e) DPW will display “No-Drone” signs at all installation entry points and any additional locations, per DES discretion.

(f) SJA will liaise with local law enforcement (LE) personnel and civilian prosecutors to identify Federal, State, and local laws and regulations related to privacy, photography, reckless endangerment, and so forth, that may be used to pursue prosecutions and/or civil penalties against UAS operators who fly aircraft over or near Army installations. Also, establish agreements with local law enforcement (LE) officials to coordinate procedures for local LE response to non-official UAS activity near installations, such as assistance in locating operators and enforcing any violations committed beyond installation boundaries.

17-3. Prohibitions.

By order of the Installation Commander privately owned Unmanned, Remote Controlled (RC), and Model (drone/quad-copters) aircraft are NOT authorized to operate over any portion of Fort Knox Military Reservation. IAW AR 95-23 UAS operation in Restricted Area R-3704 (Range Control) for recreational use is strictly prohibited. All other UAS MUST have an approved FAA Certificate of Authorization. This includes UASs for commercial use. The alternative is to join a RC flying club. There are a few in the local area: Hardin County Radio Control Modelers, Elizabethtown, KY, Louisville Radio Control Club, Louisville, KY, and Knox Model Airplane Club in Irvington, KY

Appendix A

References

Section I
Required Publications

DoDM 5100.76
Physical Security of Sensitive Conventional AA&E

DoD 5200.08
Physical Security Program

DoDD 8190.3
Smart Card Technology

DODEA AI 5705.01,Vol 1
DoDEA Force Protection Program

DODEA AI 5705.01,Vol 2
DoDEA Force Protection Program: Force Protection Conditions

DODEA AI 5705.01,Vol 3
DoDEA Force Protection Program: Physical Security

Section 797 of Title 50
The Internal Security Act of 1950, Section 21

18 USC 795
Photographing and sketching defense installations

18 USC 797
Publication and sale of photographs of defense

18 USC 1382
Entering military, naval, or Coast Guard property

50 USC 797
Penalty for violation of security regulations and orders

AR 25-22
The Army Privacy Program

AR 25-55
The Department of The Army Freedom of Information Act Program

AR 25-400-2
The Army Records Information Management System (ARIMS)

AR 40-3
Medical, Dental, and Veterinary Care

AR 40-61
Medical Logistics Policies

AR 190-11
Physical Security of Arms, Ammunition, and Explosives

AR 190-13
The Army Physical Security Program

AR 190-14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-16
Physical Security

AR 190-45
Law Enforcement Reporting

AR 190-51
Security of Unclassified Army Property (Sensitive and Non-sensitive)

AR 190-56
The Army Civilian Police and Security Guard Program

AR 195-5
Evidence Procedures

AR 380-5
Department of the Army Information Security Program

AR 380-67
Personnel Security Program

AR 385-10
The Army Safety Program

AR 600-8-14
Identification Cards For Members of The Uniformed Services, Their Family Members, and Other Eligible Personnel

AR 600-85
The Army Substance Abuse Program

AR 710-2
Supply Policy Below the National Level

AR 735-5
Property Accountability Policies

AR 870-20
Army Museums, Historical Artifacts, and Art

DA Pam 385-10
Army Safety Program

DA Pam 385-64
Ammunition and Explosives Safety Standards

DA Pam 190-51
Risk Analysis for Army Property

DA Pam 710-2-1
Using Unit Supply System (Manual Procedures)

DA Pam 750-8
Army Maintenance Management System

Air Force Instruction (AFI) 21-200
Munitions and Missile Maintenance Management

AFI 23-201
Fuels Management

FM 3.19.30 Army Tactics, Techniques, and Procedures (ATTP)
Physical Security

Fort Knox Reg 190-11-1
Privately Owned Weapons and Ammunition Control and Prohibited Weapons

Unified Facilities Criteria 4-010-01 (UFC)
DoD Minimum Antiterrorism Standards for Buildings

United States Code (USC)
Accessible through http://www.law.cornell.edu/uscode/text

Section II
Related Publications

HQDA Message on the Final Implementation of the Lautenberg Amendment to the Gun Control Act of 1968, dated 161400Z Oct 03

Army Directive 2018-07-17 (Prioritizing Efforts for Readiness and Lethality (Update 17)), dated 28 Nov 2018

Section III
Prescribed Forms

DA Form 1296
Stock Accounting Record

DA Form 1594
Daily Staff Journal or Duty Officer's Log

DA Form 2062
Hand Receipt/Annex Number

DA Form 2806-1R
Physical Security Survey Report

DA Form 3749
Equipment Receipt

DA Form 4604
Security Construction Statement

DA Form 5513
Key Control Register and Inventory

DA Form 5557
Individual Reliability Screening and Evaluation Record

DA Form 7278-R
Risk Level Worksheet

DA Form 7281
Command Oriented AA&E Security Screening and Evaluation Record

FK Form 2759-E
Registration of Privately-Owned Weapons

FK Form 210-1-1
Warning Label 0 Weapons Prohibited in Federal Buildings

SF Form 700
Security Container Information

SF Form 701
Activity Security Checklist

SF Form 702
Security Container Check Sheet

Glossary
Section I - Abbreviations

AAFES
Army and Air Force Exchange Service

BATFE
Bureau of Alcohol, Tobacco, Firearms, and Explosives

DES
Directorate of Emergency Services

DFMWR
Directorate of Family Morale, Welfare and Recreation

DoD
Department of Defense

DPW
Directorate of Public Works

GC
Garrison Commander

IACP
Installation Access Control Point

ICE
Interactive Customer Evaluation

ID
Identification

LEOSA
Law Enforcement Officers Safety Act

NCIC
National Crime Information Center

NFA
National Firearms Act

SC
Senior Commander

SJA
Staff Judge Advocate

SOP
Standard Operating Procedure

UCMJ
Uniform Code of Military Justice

USACC
United States Army Cadet Command

U.S.C.
Unites States Code

Terms

Access control
Permitting or denying the use of a particular resource by a particular entity.

Addict
Any person who habitually uses a controlled substance and has lost the power of self-control with reference to the use of controlled substance; and any person who is a current user of a controlled substance in a manner other than as prescribed by a licensed physician. Such use is not limited to the use of drugs on a particular day, or within a matter of days or weeks before, but rather that the unlawful use has occurred recently enough to indicate that the individual is actively engaged in such conduct. A person may be an unlawful current user of a controlled substance even though the substance is not being used at the precise time the person seeks to acquire a firearm or receives or possesses a firearm.

Ammunition
Projectiles combined with their fuses, propelling charges, and primers that are designed to be expelled from a firearm. This includes any type of military and commercial ammunition (ball, tracer, incendiary, blank, shotgun, black powder, and shot). Items shall only be considered as ammunition when loaded into a cartridge with its bullets, powder, and primer.

Antique firearm
A firearm designed and manufactured before 1898.Muzzleloader firearms are considered “antique firearms” and there for are not classified as firearms under the Gun Control Act of 1968 (GCA).

Armor-piercing ammunition
A projectile or projectile core which is constructed entirely (excluding the presence of traces of other substances) from one or a combination of tungsten alloys, steel, iron, brass, bronze,

beryllium copper, or depleted uranium. It is designed primarily for the purpose of penetrating metal or body armor and to be used principally in rifles, pistols and revolvers.

Automatic weapons
A firearm which continues to fire and load ammunition from its magazine as long as the trigger is depressed (or until the magazine is depleted).

Barrel
The tube, usually metal, through which a controlled explosion or rapid expansion of gases are released in order to propel a projectile out of the end at a high velocity

Cantonment area
The central portion of the Fort Knox Reservation excluding field training sites, firing ranges and hunting areas, which include commercial and government facilities and activities, installation and unit headquarters, troop billets, and family housing.

Chemical weapon
Ammunition, device or equipment, specifically designed to cause death or other harm through toxic properties which would be released as a result of the employment of such munitions or device.

Concealed weapon
Any instrument used or designed for the purpose of inflicting grievous bodily harm that is carried on the person in such a way as to be hidden from ordinary view. Folded knives with blades shorter than 3 inches are excluded from this definition.

Note: Folded knives with blades longer than 2 ½–inches in length are considered a Dangerous Weapon and are not authorized in a Federal Facility.

Controlled substance
A drug or other chemical whose manufacture, possession, or use is regulated by government and is the subject of legislative control. This may include illegal drugs and prescription medications.

Crime
An unlawful act punishable by local or federal government.

Dangerous or deadly weapon
Device, instrument, material, or substance, animate or inanimate, that is used for, or is readily capable of, causing death or serious bodily injury, except that such term does not include a pocket knife with a blade of less than 2 ½–inches in length.

Declaration of a Firearm
Declaration of a firearm at an Installation Access Control Point is identified as an immediate unsolicited acknowledgement to the Guard that you are carrying a firearms. This requires identifying where the firearms is located, the configuration in which it is carried and provide the original copy of your firearm permit.

Explosive, incendiary, and pyrotechnic device
Any type of device that is designed, made, or adapted for the purpose of inflicting serious bodily injury, death, or substantial property damage, or for the principal purpose of causing such a loud report as to cause undue public alarm or terror, and includes a device designed, made, or adapted for delivery or shooting an explosive weapon. To include military or commercial explosive, incendiary, gas (to include chemical mace) or bomb, grenade, rocket, missile, mine, blasting cap, ”dummy" and/or practice device such as simulators, and other similar detonating devices which are capable of being altered to contain a live charge, and pyrotechnic devices such as firecrackers, cherry bombs, bottle rockets, and star clusters.

Federal facility
Any building or part thereof owned or leased by the Federal Government, where Federal employees are regularly present for the purpose of performing their official duties.

Firearm
Any type of weapon which is designed or redesigned, made or remade, modified or re-modified to expel a projectile by action of an explosive force. This does not include antique firearms, antique replicas, and those modern firearms which have been rendered permanently inoperable.

Handgun
A pistol, revolver or other firearm originally designed to be fired by the use of a single hand.

Installation access control points
Locations at the outermost boundary of Fort Knox (or cantonment area) where security checks can be performed on individuals, vehicles, and materials before potential threats can gain close proximity to Army assets.

Minor
A person who has not reached the full legal age of the majority, with legally demarcates childhood from adulthood (generally 18 years of age, defined in KRS 2.015).

Misdemeanor
An offense, other than a traffic infraction, for which a sentence to a term of imprisonment of not more than twelve (12) months can be imposed.

Muzzleloader
A firearm in which the projectile and propellant charge is loaded in the front end of the barrel.

National Crime Information Center
A computerized index of criminal justice information such as criminal record history information, fugitives, stolen properties, and missing individuals. The system is operated by the FBI available to federal, state, and local law enforcement and other criminal justice agencies.

NFA firearms (Type II)
Certain firearms, explosive munitions, and other devices which are legally regulated in the United States by the National Firearms Act (NFA).

a. Machine guns and automatic weapons. Any firearm which can fire more than 1 cartridge per trigger pull. Both continuous fully automatic fire and "burst fire" (for example, firearms with a 3-round burst feature) are considered machine gun features. The weapon's receiver is by itself considered to be a regulated firearm.

b. Short-barreled rifles. Any firearm with a butt stock and a rifled-bore barrel under 16 inches long or an overall length under 26 inches. The overall length is measured with any folding or collapsing stocks in the extended position. The category also includes firearms which came from the factory with a butt stock that was later removed by a third party.

c. Short barreled shotguns. Any firearm with a butt stock and a smooth-bore barrel under 18 inches or a minimum overall length under 26.

d. Suppressors. Any portable device designed to muffle or disguise the report of a portable firearm. This category does not include non-portable devices, such as sound traps used by gunsmiths in their shops which are large and usually bolted to the floor.

e. Destructive Devices. There are two broad classes of destructive devices:

(1) Devices such as grenades, bombs, explosive missiles, poison gas weapons, etcetera;

(2) Any firearm with a bore over 0.50 inches. (Many firearms with bores over 0.50" inch, such as 12-gauge shotguns, are exempted from the law because they have been determined to have a "legitimate sporting use".)

*f. Any Other Weapons***.** This is a broad category used to regulate any number of firearms which the BATFE under the NFA enforces registration and taxation. Examples include (but not limited to):

(1) Smooth-bore pistols.

(2) Pen guns and cane guns.

(3) A firearm with combinations smooth bore and rifle barrels 12 inches or more but less than 18 inches in length from which only a single shot can be made from either barrel.

(4) Disguised firearms.

(5) Firearms that can be fired from within a wallet holster or a briefcase.

(6) A short-barreled shotgun which came from the factory with a pistol grip and no butt stock.

(7) Handguns with a forward vertical grip.

Pepper spray
Any device sold commercially for personal protection, which is designed, made, or adapted for the purpose of dispensing a substance capable of causing an adverse psychological or physiological effect on a human being.

Possession
Exercise actual dominion or control over a tangible object.

Projectile
An objected expelled by the exertion of a propellant force. The propellant may be air, an explosive solid, or an explosive liquid.

Rifle
A firearm with a rifled-bore designed to be fired from the shoulder.

Rifled-bore
A series of spiraled grooves or angles within the barrel to provide the projectile an induced spin to stabilize it.

Serious physical injury
Injury which creates a substantial risk of death, or which causes serious and prolonged disfigurement, prolonged impairment of health, or prolonged loss or impairment of the function of any bodily organ.

Shotgun
A firearm with a smooth-bore designed to be fired from the shoulder, designed to fire either a single, multiple-ball shot or a single projectile for each single pull of the trigger.

Smooth-bore
No grooves or angles are within the barrel, as the projectile is otherwise stabilized or stabilizing is undesired or unnecessary.

Stun Gun
A battery-powered, hand-held weapon that fires an electric charge when held against a person and activated by a trigger or button, to immobilize a person briefly and without injury.

Switchblade knife
A type of knife with a folding or sliding blade contained in the handle which is opened automatically by a spring when a button, lever, or switch on the handle or bolster is activated.

Taser
A stun gun that shoots prongs to deliver an electrical current to shock to a person. It uses electrical current to disrupt voluntary control of muscles causing "neuromuscular incapacitation".

Violation means an offense, other than a traffic infraction, for which a sentence to a fine only can be imposed.

Weapon
Any instrument used in an offensive or defensive manner designed to inflict damage or harm to living beings, structures, or systems.

Weapon of mass destruction
Any weapon that is designed or intended to cause death or serious physical injury through the release, dissemination, or impact of toxic or poisonous chemicals, diseases, or radiation.

Appendix B
Arms Room Close/Relocation Procedures

ARMS ROOM CLOSE OUT PROCEDURES

1. The following procedures are required by Commanders (CDRs)/Facility Managers (FM) when closing out an arms room, either temporarily or permanent:

a. The Commander/FM must make an appointment with IPSO at 624-1911 and schedule a close out inspection.

b. Place ICIDS alarm in “ACCESS” mode once the arms room has been inspected by PSS, cleared out, and no longer in use. The high security padlock will be removed and combination will be returned to the factory setting of 50-25-50.

c. Commander/FM must prepare a memorandum stating, “No sensitive items have been left in the arms room”. Memorandum must include the Building number and zone description, i.e, A, B, C, etc.

d. Commander/FM must submit memorandum to the Physical Security Division, Directorate of Emergency Services (DES) (ATTN: ICIDS Administrator), to complete close out procedures. The ICIDS Administrator is located in the DES Bldg. 298; 624-1911.

ARMS ROOM PRE-OCCUPANCY PROCEDURES

1. Contact the ICIDS Administrator at 624-1911 to ensure the activation of the ICIDS system prior to scheduling a pre-occupancy inspection.

2. Contact the Installation Physical Security Office at 624-1911 for pre-occupancy inspections.

3. Units must submit the following documents to the ICIDS Administrator to receive access to a new arms room:

a. Pre-occupancy inspection.

b. New memorandum requesting PICs for the AA&E storage facility signed by commander/FM identifying all prerequisites of AR 190-11 and AR 190-13 have been met as it pertains to personnel. Ensure all Arms Room Officer, Armorers, key control officer/custodian have been interviewed, back ground checks completed and trained on arms room and key control procedures.

c. Current copy of CDR's assumption of command memorandum.

Appendix C
ICIDS Alarm System Test Procedures

1. Monthly Walk/Duress Check. The monthly walk and duress checks will be conducted by all alarm zones and logged by the armorer or custodian, and the alarm monitor (AM).

2. Alarm systems will be tested monthly and annotated on DA form 4930 by an authorized personal identification code (PIC) holder of each facility. The custodian conducting the test must authenticate with the AM prior to entry or executing the test.

(a) They must arm the facility as though they were leaving at the end of the day, close and exit. It is imperative that the custodian wait to test door sensors and motion detectors until after the delay countdown has completed and the system is in a “SECURE” mode.

(b) After receiving a "GOOD SEAL" message from the AM, the custodian must then enter the alarmed area and activate every alarm point in the facility (this occurs as soon as the door is opened and the custodian walks around in the area); next step is to activate the Duress Switch.

(c) It is the responsibility of the AM to instruct the custodian on how to complete these tests if the custodian is unsure on the procedures. The custodian will then reset the duress by inserting the "Reset Tool" into the duress switch and removing it. When reset correctly, the AM will acknowledge that it has reset.

(d) At this point, the custodian will need to “Disarm” the system by entering their PIC, then re-enter their PIC cycling the system to “Arm” and once more back to “Disarm”; this places the system in the “ACCESS” mode.

3. Alarm/duress tests will be recorded and maintained for one year.

Appendix D
Restricted Areas

1. General

a. This appendix provides guidance on the definition, designation and prohibited actions concerning restricted areas.

b. Army installations, facilities, and operational areas of civil works and like projects are restricted areas. At a minimum the type of restriction is at the level called controlled. This is an area defined by an established boundary to prevent admission unless certain conditions or controls are met to safeguard the personnel, property or material within. These areas are not to be confused with those designated Federal Aviation Administration areas over which aircraft flight is restricted. All restricted areas will be marked and have the ability to control access to the area. Restricted areas are identified by the different types of conditions required to permit entry. Conditions for entry vary depending on the nature and degree of importance of the security interest or government assets contained within a restricted area.

c. Minimum requirements is per AR 190-13, 190-51, and this regulation.

d. Commercial imaging surveillance by photography or video recording is prohibited. Written procedures will be established and coordinated with supporting law enforcement, physical security, legal and public affairs offices, at a minimum. Procedures will establish rules for noncommercial imaging (for example, photography or video recording by Family members) and commercial imaging of events (for example, graduations and weddings).

2. Command authority

a. DODI 5200.08, per Section 797, Title 50, United States Code (50 USC 797) (Section 21 of the “Internal Security Act of 1950”), authorizes military commanders to issue regulations to safeguard DOD property and places under their command. Commanders of military installations and facilities have the authority to publish and enforcement rules.

b. The military commander in the chain of command immediately above an installation or activity that is not headed by a military commander will enforce regulations or orders pertaining to such an installation or activity issued under the authority of 50 USC 797.

3. Prohibited actions

a. A summary of pertinent sections of Title 18 of the USC follows concerning the prohibited acts announced on installation access control point (IACP) signage seen in figure 2–1 or similar.

b. Title 18 USC 795 prohibits photographing and sketching defense installations without permission.

c. Title 18 USC 797 prohibits publication and sale of photographs of defense installations without permission (this includes video).

d. Title 18 USC 1382 restricts entering or reentering military, naval, or coast guard property for any purpose prohibited by law.

4. Security procedures concerning the prohibition on commercial image collection and Surveillance

a. Commercial surveillance vehicles (mapping vehicles) are denied access to Army installations, this will be periodically validated (tested). Installation access control personnel will be on the lookout for these vehicles and will question commercial vehicle access requests in detail. Public affairs officers will be made aware that access is not to be granted in these cases.

b. Where access has been granted to a commercial organization and / or installation imagery is available on a Web site will be immediately reported.

c. Installation-level force protection working groups will be coordinated and provide situational awareness and promote a multi-disciplined approach to countering this potential threat.

5. Restricted area signs

a. Signs or notices will be posted in conspicuous and appropriate places to identify the site as a restricted area except when such action would tend to advertise an otherwise concealed area. Announcement of the site as restricted will include posting signs at each entrance to the site and on perimeter fences or other boundary material.

b. Signs will be positioned to avoid concealment of an intruder or obstruct visual assessment by friendly forces. Failure to post conspicuous signs and notices to give persons approaching a restricted area actual knowledge of the restriction may hamper any resulting legal procedure.

(1) Signs will be posted at IACPs and facility entry control points. The following declarations, individually or in combination, may be added where applicable:

(a) Deadly force authorized.

(b) Area patrolled by military working dog (MWD) teams.

(c) The introduction of weapons, ammunition, or explosives or other prohibited items and photography (including video) is prohibited without specific authorization from the commander.

6. National Defense Areas

a. A restricted area may be established on non-Federal lands within the United States and its possessions and territories to protect classified defense information and DOD equipment or material. When this type of area is established, it will be referred to as a National Defense Area (NDA). Examples of a NDA would include nuclear and chemical event sites and aircraft crash sites.

b. Establishing a NDA temporarily places such non-Federal lands under the effective control of DOD and results only from an emergency event.

c. The senior DOD representative at the scene will define the boundary, mark it with a physical barrier, and post warning signs. Every reasonable attempt will be made to obtain the landowner's consent and cooperation in establishing of the NDA. Military necessity, however, will determine the final decision regarding NDA location, shape, and size.

d. The authority to establish a NDA includes the authority to deny access to it. It also includes the authority to remove persons who threaten the orderly administration of the NDA. Any use of force employed to enforce this authority will be per AR 190–14.

7. Procedures for restricted area violations

a. The installation commander will cause any person who enters the installation or a restricted area without authority to be immediately brought before proper authority for questioning.

(1) The person may be searched per AR 190–30. Any notes, photographs, sketches, pictures, maps, or other material describing the installation or restricted area may be seized (retained). This includes but is not limited to photographic and recording devices of any type whether they be a camera, video recorder, phone, iPad, GoPro, etc.

(a) Those displaying dash mounted cameras on privately owned or commercial vehicles may remove or cover the device while on the installation.

(2) Persons brought before proper authority for questioning will be advised of their rights per AR 190–30. Questioning will be conducted without unnecessary delay.

b. If the person was unaware of the restriction, and did not acquire or intend to acquire knowledge of sensitive or classified information by entering, that person will be warned against reentry and released.

c. If it appears that the person knowingly entered a restricted area, or may have acquired or intended to acquire sensitive or classified information by entering, or may have committed some other offense, the actions below will be taken.

(1) Persons not subject to the Uniform Code of Military Justice will be taken to civilian law enforcement officials. In the United States, the nearest office of the FBI will be notified and the person will be turned over to the nearest U.S. marshal. If the person cannot be turned over to a U.S. marshal within a reasonable period of time (generally 3 to 4 hours), the person will be taken before an appropriate state or local official (see 18 USC 3041). As soon as possible, the agency to which the person is transferred will be given a written statement of facts with the names and addresses of witnesses and pertinent exhibits as may be available.

(2) A person subject to the Uniform Code of Military Justice will be turned over to their commander or the proper military law enforcement official.

d. MPI/ MI/ CI may be contacted. However, any unauthorized photographic activity will be reported to the Provost Marshal Office at 624-7093.

e. Facts concerning a deliberate violation of a restricted area will be immediately reported per AR 381–12.

Appendix E
Personnel Reliability Program

a. Determining reliability. The following positions or duties in Army physical policies require a determination of reliability—

(1) Unaccompanied access to arms, ammunition, and explosives per AR 190-11.

(2) Unaccompanied access to controlled medical substances per AR 190-51.

(3) Employment and retention as a DA police officer or DA security guard, per AR 190-56.

b. Commander or director’s program. Determining personnel reliability is a commander or director's program. Commanders and directors must be aware of, and concerned with, the reliability at all times of personnel having unaccompanied access to identified areas. A total team effort and interaction is necessary for this program to be successful.

c. Delegation of authority. The responsibility for this program may be delegated to the level of supervision best suited to evaluate program members on a continuing basis. When authority is delegated, the commander or director retains the responsibility to review decisions to qualify or disqualify personnel. The commander or director will issue a written delegation of authority, by memorandum, for a certifying official who will have responsibility for the determination process.

d. Inherently governmental. A decision concerning the reliability of personnel for this duty is inherently a governmental function. Contractors cannot certify their own personnel into these programs. Contractors can be assigned as monitors to help the certifying official continue to evaluate personnel, but ultimately the decision to qualify or disqualify rests with the commander or director, by means of the delegated certifying official.

e. Supporting form. The DA Form 7708 (Personnel Reliability Screening and Evaluation Form), with instructions on use in appendix E, is used to document the reliability determination process as follows—

(1) Personnel data. This includes the Social Security number.

(2) Personnel records check. A qualified personnel official will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information.

(3) Security records check. A security clearance is not required for unaccompanied access to arms, ammunition, explosives, and controlled medical substances. The commander or director may, however, use this check as an additional determination factor. If a security records check is conducted, the reviewing security official will

electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information, in the official's judgment.

(1) Medical records check. The reviewing competent medical authority (a licensed physician, physician's assistant, or nurse practitioner) will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information in the official's judgment. A DD Form 2870 (Authorization for Disclosure of Medical or Dental information) is required if the records are retained by a non-DOD medical entity. A person is immediately disqualified from the position, or duty, under consideration if the person does not provide such authorization.

(2) Law enforcement records check. This check will be conducted by the supporting Army law enforcement office by a query of the Army Law Enforcement Reporting and Tracking System. A senior law enforcement official will electronically annotate on the DA Form 7708 if the records contain potentially disqualifying information, in the official's judgment.

(3) Drug test. A drug test may or may not be required for the PSO and PSI positions and duties. The commander or director may, however, use this check as an additional determination factor. If a drug test is used, a qualified test official will electronically annotate on the DA Form 7708 if the test results in potentially disqualifying information. The DA Form 7708 provides for drug testing results if other policy proponents use the form and need such information.

(4) The supervisor briefing to a prospective person.

(5) Continuing periodic evaluations of an incumbent person.

(6) Suspension or temporary disqualification of an incumbent person.

(7) Disqualification of an incumbent person.

f. Responsibility to inform. Supervisors at all levels have an inherent responsibility to inform the commander or director about all cases of erratic performance or poor judgment by personnel, on or off duty that could affect duty reliability. All personnel are responsible for reporting to their immediate supervisor any behavior that might affect a co-worker's reliability.

g. Continuous evaluation. It is essential to continually evaluate personnel in this program. Any incident or problem that might be cause for temporary or permanent removal from the program must be promptly reported to the certifying official and supervisors. Those providing medical care and maintaining medical records are required to report any incident or allegation about a person's suitability under this program. Verbal or telephonic notifications will be confirmed in writing.

h. Documenting behavior patterns. To ensure commanders and directors are aware of patterns of behavior that may indicate unreliability, commands and activities should establish a documentation system. It would document discipline of employees, in both

supervisor and employee records. These records will be periodically reviewed by certifying officials.

i. Potential duty impairment. Personnel have a continuous responsibility to report all medical treatment and medication that may impair their ability to perform the essential functions of the job to the competent medical authority as it occurs, regardless of whether the treatment was provided through the federal health system or by a private health care provider. The examining physician will make a recommendation to the certifying official concerning the potential impact of the condition, treatment, or medication on reliability. If the examining physician is not in Federal service, then the evaluation findings and the examining physician's recommendation must be forwarded to a physician having Federal status for review and approval.

j. Personnel interview. The certifying official will interview the person to appraise character, judgment, reliability, attitude, emotional and mental maturity, and sense of responsibility. Personnel exhibiting financial irresponsibility will not be selected. The interview will be documented on DA Form 7708, which will be completed per appendix E of this regulation.

k. Annual review. The reliability determination will be reviewed every year in the on-boarding month or upon change of status (for example, departs the unit, criminal activity whether alleged or adjudicated).

Appendix F
Instructions for Completing the DA Form 7708

1. Purpose
This regulation provides instruction to use the DA Form 7708 (Personnel Reliability Screening and Evaluation). The purpose of the form is to help review records to determine the suitability of a person to perform a certain duty assignment or gain access to certain materials. Examples of duty assignments include, but are not limited to physical security inspectors and DA civilian police and security guards. Examples of access to certain materials include, but are not limited to, unaccompanied access to arms, ammunition, explosives, and controlled medical substances. The DA Form 7708 is available for any Army policy proponent having duty assignments that warrant a greater degree of suitability determination than provided for civilian employees upon entry and Soldiers upon accession to the U.S. Army.

2. General
a. The DA Form 7708 is designed for electronic signatures, and is also intended to be transmitted and stored as an electronic document.

a. Emails that electronically transmit the DA Form 7708 will include an electronic signature to verify the sender, and also digital encryption to protect personally identifiable information.

b. The Social Security number is used to retrieve correct medical and law enforcement records.

d. A paper copy of the DA Form 7708 is authorized, if necessary. The form will be protected at all times while in use or being hand-carried to protect personally identifiable information.

e. The DA Form 7708 provides for eight personnel roles.

(1) The individual.

(2) The supervisor of the individual.

(3) The certifying official.

(4) The reviewing official.

(5) A supporting personnel official.

(6) A supporting security officer.

(7) A supporting competent medical authority.

(8) A supporting law enforcement authority

f. The DA Form 7708 will be retained for record until such time the individual is no longer associated with the command.

3. Potentially disqualifying information
Information that is adverse to the individual may be revealed during checks of required records. Information that could potentially disqualify a person from a specific duty will vary. An example is medical information that could indicate a condition that poses a safety risk for one duty but is suitable for another duty. Records reviewing officials will consider the nature and elements of the duty for which the individual is being considered, and provide a professional assessment to the interviewer. The interviewer will consider all information as a whole and make an informed decision. The DA Form 7708 is marked For Official Use Only, due to the presence of personally identifiable information.

4. Completing the DA Form 7708
The DA Form 7708 will be used to screen and evaluate personnel reliability of physical security inspectors, per paragraph 2–21. The interview must complete part I prior to parts II through VI. Part VII will only be completed once parts II through VI are completed as required.

a. Part I: Immediate supervisor, commander, or director interview.

(1) Block 1. Enter the name of the interviewed individual.

(2) Block 2. Enter the organization.

(3) Block 3. Enter position title.

(4) Block 4. Enter the person’s Social Security number.

(5) Block 5. The person will check one of the two blocks. The interview process will be terminated if the person indicates objection to the screening requirements. The certifying official will record the objection in blocks 49 and 50.

(6) Block 6. Check the applicable block for the pending duty. If the duty is not listed, use the “other” block and specify the duty.

(7) Block 7. The person will electronically sign the form in this block.

(8) Block 8. The date is automatically applied when Block 7 is signed

(9) Block 9. Enter the name of the interviewer.

(10) Block 10. The interviewer will electronically sign the form in this block

(11) Block 11. The date is automatically applied when Block 10 is signed.

b. Part II: Check of personnel records.

(1) Block 12. The reviewing personnel official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.

(2) Block 13. The reviewing personnel official will enter their name.

(3) Block 14. The reviewing personnel official will electronically sign the form in this block.

(4) Block 15. The date is automatically applied when Block 14 is signed.

c. Part III: Check of security records.

(1) Block 16. The reviewing security official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.

(2) Block 17. The reviewing security official will enter the date of the personnel security adjudication, the type of investigation, if the adjudication was favorable, or if the dossier requires a review.

(3) Block 18. The reviewing security official will enter the date and type of investigation, if a personnel security investigation or reinvestigation was requested.

(4) Block 19. The reviewing security official will indicate the level of security clearance.

(5) Block 20. The reviewing security official will enter their name in this block.

(6) Block 21. The reviewing security official will electronically sign the form in this block.

(7) Block 22. The date is automatically applied when Block 21 is signed.

d. Part IV: Check of medical records.

(1) Block 23. The reviewing medical official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.

(2) Block 24. The reviewing medical official will enter their name.

(3) Block 25. The reviewing medical official will electronically sign the form in this block.

(4) Block 26. The date is automatically applied when Block 25 is signed.

e. Part V: Check of law enforcement records.

(1) Block 27. The reviewing law enforcement official will check one of the two blocks, indicating whether potentially disqualifying information was or was not found.

(2) Block 28. The reviewing law enforcement official will enter their name.

(3) Block 29. The reviewing law enforcement official will electronically sign the form in this block.

(4) Block 30. The date is automatically applied when Block 29 is signed.

f. Part VI: Results of random or directed drug testing.

(1) Block 31. The reviewing drug-testing official will check one of the two blocks, indicating whether potentially dis-qualifying information was or was not found.

(2) Block 32. The reviewing drug-testing official will enter their name.

(3) Block 33. The reviewing drug-testing official will electronically sign the form in this block.

(4) Block 34. The date is automatically applied when Block 33 is signed.

g. Part VII: Immediate supervisor, commander, or director’s evaluation or briefing.

(1) Block 35. After reviewing all provided records, the certifying official making the informed decision that the individual is suitable for the duty will check one of the two blocks. The certifying official will brief the individual on the duties and standards.

(2) Block 36. The person will read this statement.

(3) Block 37. The person will affirm an understanding of the duties and standards by electronically signing the form in this block.

(4) Block 38. The date is automatically applied when Block 37 is signed.

(5) Block 39. Enter the name of the certifying official (interviewer).

(6) Block 40. The certifying officer will electronically sign in this block.

(7) Block 41. The date is automatically applied when Block 40 is signed.

h. Part VIII: Continuing periodic evaluation.

(1) Block 42. The person will electronically sign the form in this block.

(2) Block 43. The certifying official will electronically sign the form in this block.

(3) Block 44. The certifying official will enter relevant comments in this block.

i. Part IX: Suspension or temporary disqualification. Block 45. The certifying official will enter the date in this block. The certifying official will annotate information about the suspension or disqualification in Part VIII.

j. Part X: Administrative termination. Block 46. The certifying official will enter the date in this block. The certifying official will annotate information about the administrative termination in Part VIII.

k. Part XI: Disqualification.

(1) Block 47. The certifying official will annotate the status of the individual at the time of the disqualification in this block.

(2) Block 48. The certifying official will annotate the reason for the disqualification in this block, and use Block 50 as the reason, if other than the listed reasons.

(3) Block 49. The certifying official will check this block to indicate the individual is disqualified.

(4) Block 50. The certifying official will annotate the rationale for disqualifying the individual in this block.

(5) Block 51. The certifying official will annotate the date the person was notified of the disqualification and the means of notification in this block.

(6) Block 52. Enter the name of the certifying official.

(7) Block 53. The certifying official will electronically sign the form in this block.

(8) Block 54. The date is automatically applied when Block 53 is signed.

(9) Block 55. Enter the name of the reviewing official.

(10) Block 56. The reviewing official electronically signs the form in this block.

(11) Block 57. The date is automatically applied when Block 56 is signed.

Glossary

Section I
Abbreviations

A&E
arms and explosives

AA&E
arms, ammunition, and explosives

AAFES
Army Air Force Exchange Service

ACP
access control point

AIE
Automated Installation Entry

AIT
automatic identification technology

ALSE
aviation life support equipment

AM
alarm monitor

AMC
Army Materiel Command

AMDF
Army Master Data File

ANCIC
access national agency check with written inquiries

AR
Army regulation

ARO
arms room officer

ASL
authorized stockage list

ASP
ammunition supply point

AT/FP
antiterrorism/force protection

AWOL
absent without leave

BDE
Brigade

BMS
Balance magnetic switch

BN
battalion

CAC
common access card

CAT
category

CBRNE
chemical, biological, radiological, nuclear and explosive

CCTV
closed-circuit television

CDR
Commander

CCIR
Commanders Critical Information Requirements

CoC
chain of command

COMSEC
communications security

Co
company

CP
crime prevention

CPO
Crime Prevention Officer

CQ
charge of quarters

DA
Department of the Army

DASA
deployment ammunition storage area

DASG
Department Army Security Guard

DECA
Defense Commissary Agency

DES
Directorate of Emergency Services

DFMWR
Directorate of Family, Morale, Welfare, Recreation

DIR
director

DL
drivers license

DLA
Defense Logistics Agency

DoD
Department of Defense

DoDEA
Department of Defense Education Activity

DoDIC
Department of Defense Identification Code

DOT
Department of Transportation

DPBO
Director of Property Book Office

DPTMS
Directorate of Plans, Training, Mobilization and Security

DPW
Directorate of Public Works

DRC
Directorate Readiness Center

DWI
driving while intoxicated

EOD
explosive ordnance disposal

ETS
expiration term of service

FLMSA
field level munitions storage area

FM
facility manager

FORSCOM
United States Army Forces Command

FOUO
For Official Use Only

FPCON
force protection condition

FPO
Force Protection Officer

GC
Garrison Commander

GRP
group

GS
General Schedule

GSA
General Service Administration

HC
host commander

HQDA
Headquarters Department of the Army

HRT
high risk target

HSP
high security padlock

IACP
installation access control point

IAW
in accordance with

IBA
interceptor body armor

IC
Installation Commander

ICAM
improved chemical agent monitor

ICIDS
Integrated Commercial Intrusion Detection System

ID
identification

IDG
Installation Design Guide

IDS
intrusion detection system

IG
Inspector General

IMCOM
Installation Management Command

IPPBO
Installation Property Book Officer

IPSO
Installation Physical Security Office

IRP
Individual Reliability Program

I2MC
Integrated Incident Management Center

JROTC
Junior Reserve Officers' Training Corps

LAR
Logistics Assistance Representative

MAL
master authorization list

MOA
memorandum of agreement

MOU
memorandum of understanding

MEVA
mission essential vulnerable area

MFR
memorandum for record

MP
Military Police

MWD
Military Working Dog

NBC
nuclear, biological, chemical

NCO
Noncommissioned officer

NCIC
National Crime Information Center

NCOIC
noncommissioned officer in charge

NLETS
National Law Enforcement Telecommunications System

NSN
national stock number

NVD
night vision device

OCIE
organizational clothing and individual equipment

OIC
officer in charge

PACS
Physical Security Access Control System

PAO
Public Affairs Officer

PBO
Property Book Officer

PBUSE
Property Book Unit Supply Enhanced

PCS
permanent change of station

PIC
personal identification code

PKI
public key infrastructure

PM
Provost Marshal

PMO
Provost Marshal Office

POA
privately owned ammunition

POV
privately owned vehicle

POW
privately owned weapon

PPSM
physical protective security measures

PSCPO
Physical Security and Crime Prevention Officer

PSM
physical security measure

PSO
Physical Security Officer

PSCPOC
Physical Security/ Crime Prevention Officer Course

PSP
Physical Security Plan

PSS
Physical Security Specialist

QASAS
Quality Assurance Specialist Ammunition Surveillance

RAM
random at measures

RBC
Readiness Business Center

SBE
stay behind equipment

SBP
stay behind property

SC
Senior Commander

SCIF
Sensitive Compartmented Information Facility

SDNCO
staff duty noncommissioned officer

SDO
staff duty officer

SF
standard form

SIR
serious incident report

SJA
Staff Judge Advocate

SMS
Security Management System

SOP
standing operating procedures

SQDN
squadron

TACOM
Tactical Army Command/Theater Army Command

TTP
Trusted Traveler Program

UCMJ
Uniformed Code of Military Justice

UFC
Unified Facilities Criteria

US
United States

USAMP
Unites States Army Military Police

USASOC
United States Army Special Operations Command

USC
United States Code

VCC
visitor control center

VCIF
vehicle cargo inspection facility

Section II
Special Abbreviations and Terms

Bulk Storage
Storage in a facility above the using or dispensing level specifically applicable to logistics warehouses and depot stocks. This applies to activities using controlled medical substances and items, (pharmacies, wards, or clinics) only when a separate facility (e.g., building or room) is used to store quantities that exceed normal operating stocks.

Controlled Medical Substance
A drug or other substance, or its immediate precursor, listed in current schedules of 21 USC 812 in medical facilities for the purpose of military treatment, therapy, or research. Categories listed in this section are narcotics, amphetamines, barbiturates, and hallucinogens.

Installation Access Control Procedures
Standardized access control requirements for entering Fort Knox, North Carolina relating to vehicle and personnel screening, ID documents, vehicle registration, long term access control card, and temporary passes in IAW AR 190-13, chapter 8.

Motor Pool
A group of motored vehicles used as needed by different organizations or individuals and parked in a common location when not in use. On an Army installation, all units/activities to include non-tenant units with 10 or less assigned commercial-type vehicles with no local organizational maintenance support does not have a motor pool, under this regulation, even though the vehicles are parked together.

Motor vehicle
A self-propelled, boosted, or towed conveyance used to transport a burden on land. This includes all Army wheeled, tracked vehicles, trailers, and semi-trailers.
Note/Comment

Describes conditions or actions affecting the overall security, i.e. description of waivers/exceptions and the fact that compensatory measures are fully implemented by the unit/activity. A MFR signed by the CDR/DIR/FM does not negate the deficiency.

Note C Controlled Medical Items
Sets, kits and outfits containing one or more component Note Q or R items.

Note Q Controlled Medical Items
All standard drug items identified as Note Q in the Federal Supply Catalog, Non-standard Drug Enforcement Administration (DEA) Schedule III, IV, V Controlled Substances.

Note R Controlled Medical Items
All items identified as Note R in the Federal Supply Catalog, Non-standard DEA Schedule II Controlled Substances.

Observation
A condition where regulatory guidance is nonexistent, or is unclear, or is found to be a weakness in a unit's/activity's security posture.

Physical Security Measures (PSMs)
Physical security measures are designed to detect, deter, delay, and defend against threats to US Forces assets. Physical security measures are a combination of active or passive systems, devices, and security personnel. Measures may be physical (i.e., barriers, fences, lights, walls), electronic (i.e., alarms, cameras, electronic entry/access control systems, and procedural (i.e., security checks, inspections and surveys, security training and awareness programs, property inventory and accountability procedures).

Protective Seal
A protective seal is a closure device that serves as a check against tampering or unauthorized opening. If designed and attached properly a seal will show signs of tampering/forced entry.