

**XVIII Airborne Corps and Fort Liberty
Regulation 190-13-1**

Military Police

**FORT LIBERTY
PHYSICAL
SECURITY
PROGRAM**

**Headquarters
XVIII Airborne Corps and Fort
Liberty Fort Liberty, NC
29 June 2023**

SUMMARY of CHANGE

XVIII Airborne Corps and Fort Liberty Regulation 190-13-1

Fort Liberty Physical Security Program

This major administrative revision supersedes XVIII Airborne Corps and Fort Bragg Regulation 190-13-1, Fort Bragg Physical Security Program dated 12 Jan 2021.

- o Makes administrative changes (throughout).
- o Makes changes to installation pass expiration dates (throughout).
- o Makes changes to installation Physical Security forms (throughout).
- o Adds requesting a visitor pass for Foreign National Visitors (Not On Military Orders) Chapter 10-2. s.

Headquarters
XVIII Airborne Corps and Fort
Liberty Fort Liberty, NC
29 June 2023

***XVIII Airborne Corps and Fort Liberty
Regulation 190-13-1**

Effective 29 June 2023

Military Police

Fort Liberty Physical Security Program

By Direction of the Senior
Commander:



CHRISTOPHER T. DONAHUE
Lieutenant General, U.S. Army
Commanding

OFFICIAL:

BATTLE.THOMAS.
DONNELL.1047150
740

Digitally signed by
BATTLE.THOMAS.DONNELL.10
47150740
Date: 2023.08.11 16:15:04 -0400'

THOMAS D. BATTLE
Director of Human

Resources - Fort Liberty

History. This regulation supersedes XVIII Airborne Corps and Fort Bragg Regulation 190-13-1, dated 12 Jan 2021.

Summary. This regulation incorporates comments and recommendations provided since the previous publication dated 12 JAN 2021. This revision address changes in regulations, policy, terminology, and updates applicable Fort Bragg Forms to Fort Liberty.

Applicability. This regulation applies to Department of Defense (DoD) employees, contractors and all units, organizations or activities assigned, attached or tenant to Fort Liberty. Questions concerning the applicability and interpretation of contents should be referred to the Directorate of Emergency Services (DES) (ATTN: Physical Security Office).

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.

Proponent and exception authority. The proponent agency for this regulation is the Physical Security Office, DES, (AMIM-LIL-S), Fort Liberty, NC 28310-5000

Restrictions. 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, and is limited for official Government use only.

Suggested Improvements. Users are encouraged to send comments and suggested improvements directly to Director, DES (ATTN: Physical Security Office, (AMIM-LIL-S).

Distribution. This publication is available in electronic media only.

Contents

Chapter 1
General, page 1

*This regulation supersedes XVIII Airborne Corps and Fort Bragg Regulation 190-13-1, dated 12 January 2021.

Contents – Continued

Purpose • 1-1, *page 1*
References • 1-2, *page 1*
Explanation of Abbreviations and Terms • 1-3, *page 1*
Installation Physical Security Office (IPSO) • 1-4, *page 1*
Disciplinary Actions • 1-5, *page 1*
Security of Unclassified Government Property (Sensitive and Non-Sensitive) • 1-6, *page 1*
Responsibilities • 1-7, *page 1*

Chapter 2

Physical Security Planning, *page 4*

Installation Physical Security Inspections • 2-1, *page 4*
Inspection Requirements • 2-2, *page 5*

Chapter 3

Arms, Ammunition and Explosives (AA&E), *page 6*

Arms Room Standing Operating Procedures (SOP) • 3-1, *page 6*
Arms Room Bi-Lateral/Consolidated Storage Agreements • 3-2, *page 6*
Arms Room Security Lighting • 3-3, *page 7*
Arms Racks and Security Containers • 3-4, *page 7* Use
of Digital Arms Room Systems • 3-5, *page 7* Security
of Armorer Tools • 3-6, *page 8*
Contract Guard Weapons • 3-7, *page 8*
Foreign Weapons • 3-8, *page 8* Arming of
Unit Armorers • 3-9, *page 8*
Security of Non-AA&E Items • 3-10, *page 8*
Privately Owned Weapons (POWs) • 3-11, *page 10*

Chapter 4

Administrative Requirements, *page 10*

Personnel Reliability Screening and Evaluation (DA Form 7708) • 4-1, *page 10* Property
Book Officer (PBO) Monthly Sensitive Items Inventories • 4-2, *page 11* Weapons and
Sensitive Items Register • 4-3, *page 11*
Master Authorization List (MAL) • 4-4, *page 12* Department of
the Army Equipment Receipt • 4-5, *page 12* Weapons Issue
and Turn-in Procedures • 4-6, *page 13*
Arms, Ammunition and Explosives Key Control • 4-7, *page 13*
Standard Form (SF)-700, Security Container Information Sheet, • 4-8, *page 15*
SF-702, Security Container Check Sheet, • 4-9, *page 16*
Department of Army Form 4604, Security Construction Statement • 4-10, *page 16*
Required Signage • 4-11, *page 16*
Unaccompanied Access Rosters • 4-12, *page 17*
Physical Security and Crime Prevention Officer's Course • 4-13, *page 17*

Chapter 5

Administrative Key and Lock Control, *page 17*

Key and Lock Custodians • 5-1, *page 17*
Key Control Register • 5-2, *page 18* Key
Depositories • 5-3, *page 18*
Locks • 5-4, *page 18*
Electronic Card Access Accountability • 5-5, *page 19*
Protective Seal Control • 5-6, *page 20*

Contents – Continued

Chapter 6

Integrated Commercial Intrusion Detection System (ICIDS), page 21

Intrusion Detection System (IDS) Alarms • 6-1, page 21

Alarm Activations • 6-2, page 21

Alarm Tests • 6-3, page 21

Personal Identification Code (PIC) • 6-4, page 21

Security Breach of Arms Rooms/Sensitive Items Storage Areas • 6-5, page 22

Intrusion Detection System Failure Procedures • 6-6, page 22

Intrusion Detection System Work Orders • 6-7, page 22

Chapter 7

Security of Unit Motor Pools, page 23

Commander (CDR)/Director (Dir)/Facility Manager (FM) and Contractor Responsibilities • 7-1, page 23

Requirements • 7-2, page 23

Perimeter Fencing and Lighting • 7-3, page 24

Key and Lock Control • 7-4, page 24

Security of Tool Rooms/Tools • 7-5, page 24

Repair Parts not at Installation Level Supply Support Activities and Direct Support Units with an Authorized Stockage List (ASL) • 7-6, page 25

Chapter 8

Lost/Stolen Military AA&E and Other Sensitive Items, page 25

General • 8-1, page 25

Serious Incident Reporting (SIR) • 8-2, page 25

Types of Sensitive Items • 8-3, page 26

Chapter 9

Crime Prevention, page 26

Responsibilities • 9-1, page 26

Health and Welfare Inspections • 9-2, page 29

Dayroom/Barracks • 9-3, page 29

Light Control Measures • 9-4, page 30

Security During Deployments • 9-5, page 30

Chapter 10

Installation Access Control Procedures, page 30

Policy • 10-1, page 30

Procedures • 10-2, page 30

Special Event Access • 10-3, page 39

Chapter 11

Personnel Reliability Program, page 40

Program • 11-1, page 40

Delegation of Authority • 11-2, page 40

Contractors • 11-3, page 40

Instructions and use of the DA Form 7708 • 11-4, page 40

Responsibility to inform • 11-5, page 40

Continuous evaluation • 11-6, page 41

Documenting behavior patterns • 11-7, page 41

Potential duty impairment • 11-8, page 41

Personnel interview • 11-9, page 41

Annual review • 11-10, page 41

Contents – Continued

Chapter 12

Security of Aircraft and components, *page 41*

Appendixes

- A. References, *page 42*
- B. Alarm System Test Record, *page 46*
- C. Sample Appointment Order for Unit Crime Prevention Officer, *page 47*
- D. Sample Unit Crime Prevention Program SOP, *page 48*
- E. Crime Prevention Briefing Checklist, *page 50*
- F. Arms Room Closeout/Pre-Occupancy Procedures, *page 51*
- G. Controlled Substance Record, *page 52*
- H. Stock Accounting Record, *page 53*
- I. Intrusion Detection System (IDS) Personal Identification Code (PIC) Request Form, *page 54*
- J. Special Event Access Attendee List, *page 56*
- K. Physical Security Inspection Program, *page 57*
- L. Integrated Commercial Intrusion Detection System Alarm System Test Procedures, *page 59*
- M. AA&E Pre-Deployment/Reintegration Procedures, *page 60*
- N. Request for a Fort Liberty Access Control Pass (DES Form 118), *page 61*
- O. Restricted Areas, *page 62*
- P. Weapons and Ammunition Control Sheet/Log, *page 66*
- Q. Monthly Serial Number of Weapons and Ammunition (cont'd), *page 67*
- R. Weapons, Ammunition, Sensitive Items, and Key Count/Inventory, *page 68*
- S. Fort Liberty Local Records Check request form, *page 69*
- T. Use and instructions for the DA Form 7708, *page 70*
- U. Operating Civilian or Privately Owned Radio Controlled (RC) Model Aircraft/Drones/Small Unmanned Aircraft Systems (UASs) on Fort Liberty, *page 72*
- V. Duty Appointment Example, *page 73*

Glossary

Section I Abbreviations, *page 74*

Section II Special Abbreviations and Terms, *page 82*

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 Liberty includes Camp Mackall, Linden Oaks, Pope Field, and Simmons Army Airfield. This regulation is intended to provide additional physical security guidance otherwise not covered in existing Army regulations and directives.

1-2. References. Required and related publications and prescribed and referenced forms are listed in app 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 training for personnel with duties related to arms, ammunition, and explosives (AA&E), and the security of unclassified government Army and Air Force property (sensitive and non-sensitive).

f. Supporting the XVIII Airborne Corps Inspector General (IG), Quality Assurance Specialist Ammunition Surveillance (QASAS), and Installation Safety Program.

g. Conducting United States (US) Customs missions.

1-5. Disciplinary Actions.

a. Parts of this regulation are punitive. 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 criminal 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 the US Magistrate and the US District Court, as appropriate, for violation of any state laws, committed entirely or in part on Fort Liberty. Violators will be cited on Department of Defense (DD) Form 1805, Central Violation Bureau citation by recording the specific para or section of the North Carolina statute violated.

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.

1-7. Responsibilities.

a. Garrison Commander (GC). The GC will ensure physical security regulatory requirements are implemented on Fort Liberty in support of this regulation to include identifying and prioritizing physical

security resource requirements based on threat, vulnerabilities, regulatory guidance, and command directives.

b. Director of Emergency Services (DES). The DES will:

(1) Ensure Crime Prevention Programs complement the Installation Physical Security/Crime Prevention (PSCP) Program.

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

(3) Assess installation physical security needs by conducting an Installation Physical Security Survey (IPSS) every three (3) years.

c. Brigade (BDE)/Group (GRP)/Battalion (BN)/Squadron (SQDN)/DIR will:

(1) Develop a Physical Security Plan (PSP) reference AR 190-11 and provide a copy to the IPSO for inclusion into the IPSP.

(2) Develop written Standing Operating Procedures (SOP) for Crime Prevention and Physical Security.

(3) Develop and implement Physical Security SOPs which include security responsibilities for the receipt, utilization, and accountability of government AA&E/sensitive items property within their unit/activity.

(4) Establish periodic inspections of their subordinate units/activities.

(5) Assess and account for property in accordance with (IAW) with regulatory requirements.

(6) Ensure personnel directly responsible for AA&E and sensitive items attend the Arms Room Operations Course (AROC).

(7) Ensure personnel assigned and or directly responsible for Physical Security/Crime Prevention attend the Physical Security/Crime Prevention Officer Course (PSCPOC).

d. Physical Security Officer (PSO) will:

(1) Be appointed in writing by the BDE/GRP/BN/SQDN/Co level (i.e., Co, Battery, Troop, Flight) CDR, DIR or FM.

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

(3) Attend the PSOCPC within six (6) months of assignment.

(4) The BDE/GRP/BN/SQDN/DIR/FM PSOs will:

(a) Coordinate physical security inspections through the unit S2/S3 and the IPSO, (910) 396-9109.

(b) Conduct quarterly 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/FM.

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

(d) Conduct crime prevention inspections and report findings of subordinate units to the CDR/DIR/FM.

(e) Advise CDR/DIR/FM on information which may impact crime trends.

(f) Ensure Staff Duty Officer (SDO) and/or Staff Duty Noncommissioned Officers (SDNCO) conduct random checks of barracks, unit areas, equipment storage areas, and parking lots during hours of darkness. Staff Duty Officer/SDNCO journals will be maintained on file for a minimum of 90 days.

e. Arms Room Officer, Officer in Charge (OIC), and Noncommissioned Officers in Charge (NCOICs) will:

(1) Be a commissioned officer, warrant officer or an E-5 and above, or DA Civilian equivalent.

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

(3) Attend the AROC within six (6) months of assignment.

(4) Have a completed DA Form 7708 and be issued a Personal Identification Code (PIC) prior to assuming duties and will perform duties as an armorer if on unaccompanied access roster.

(5) Familiarize themselves with references in Appendix (app) A of this regulation. Note: Supply personnel (those directly working in a supply role) should not be appointed as Arms Room Officers (ARO).

f. Unit Armorers will:

(1) Will be appointed in writing by the CDR, as primary and alternate armorers.

(2) Attend the AROC within six (6) months of assignment.

(3) Have a completed DA Form 7708 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) Sub-hand receipt for all AA&E/sensitive items stored in the arms room from the CDR/DIR/FM.

(5) Become familiar with applicable references in app A of this regulation.

(6) Be strictly prohibited from conducting or participating in monthly inventories, will serve in an observation role only and are prohibited from being assigned as a key custodian.

g. AA&E Key and Lock Custodians will:

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

(2) Have a completed DA Form 7708 prior to assuming duties.

(3) Be familiar with applicable references in app A of this regulation.

(4) Attend AROC within six (6) months of assuming duties.

h. Inventory Officer for Monthly Sensitive Items Accountability will:

- (1) Be selected by the CDR/DIR/FM.
- (2) Be a non-commissioned officer (NCO), commissioned officer, warrant officer, or a DA Civilian equivalent.
- (3) Be strictly prohibited from conducting consecutive monthly inventories.

Chapter 2

Physical Security Planning

2-1. 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.
- b. Physical Security inspections will be conducted:
 - (1) In accordance with AR 190-13, para 2-15 and this regulation.
 - (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, multiple-customer automated data processing (ADP) service-center activities/facilities, and dining facilities.
 - (7) Every 24 months for MEVAs other than those listed in para (5) and (6) above.
 - (8) All other activities, to include the Directorate of Emergency Services (DES), Army Air Force Exchange Service (AAFES), Directorate of Family, Morale, Welfare and Recreation (DFMWR), and Defense Commissary Agency (DECA) will be inspected every 24 months. Facilities storing AA&E will be inspected every 18 months.
- c. Courtesy inspections will not be conducted in lieu of formal inspections.
- d. Request for changes to dates of a scheduled inspection must be submitted by the organization's first Colonel/O6 or equivalent in their chain of command and forwarded to the IPSO for approval.
- e. Installation Physical Security Office PSS will provide S2/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.
- f. Discretion to make on-the-spot corrections lies with the IPSO PSS.

g. CDRs/DIRs/FMs 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. Deficiencies beyond the capability of the CDR/DIR/FM to correct, due to a lack of resources, will be reported to the next higher CDR with a request for resource assistance, listing justification, and an impact statement.

i. Fort Liberty Physical Security inspection checklists or DA Form 2806-1-R or both will be used to prepare and record all physical security inspections.

j. DA Form 2806-1-R:

(1) Units or activities storing AA&E and SI and which receive a "Not Adequate" rating on an Installation Physical Security Inspection will submit a corrective actions memorandum (memo) to the IPSO (ATTN: Physical Security Officer) within 45 consecutive days after the initial inspection. The corrective actions memo must be received before a re-inspection can be scheduled. Re-inspections will be conducted no later than 180 days from the date of initial inspection without the approval of the IPSO.

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

(3) The IPSO will electronically forward inspection results to the inspected unit within 30 working days, and an out brief within 45 working days after the inspection. Copies of physical security inspection reports will be provided to the BDE/GRP CDRs, DIRs, FMs, and S2 Security Managers.

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

2-2. Inspection Requirements.

a. Inspection ratings will be recorded on inspection checklists, available from the Installation Physical Security Inspectors and on the Installation Physical Security Web Page. Inspections will be conducted by a credential-bearing PSS every 18 months for all arms storage facilities. Arms rooms 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 by asterisks on inspection checklists.

(2) The number of minor deficiencies noted on the checklist IAW with functional area. Minor 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, (i.e., motor pools, arms rooms, etc.). Examples of minor 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) Failure to submit required work orders immediately for deficiencies that cannot be corrected at unit/activity level.

b. Re-inspections:

(1) The Physical Security Office has the authority to inspect all AA&E facilities, Ammunition Storage Point sites, Deployment Ammunition Storage Area (DASA), Division Readiness Cage (DRC), ranges, and the transit/movement of AA&E to include control, accountability, and security on an unannounced basis.

(2) Reports will be forwarded through command channels to the CDR/DIR/FM.

(a) CDRs, DIRs, and FMs will reply in writing IAW para 2-3 of this regulation.

(b) Once the document is received, units/activities will coordinate with the Physical Security Office at (910) 396-9109, to schedule re-inspections.

(c) Re-inspections for AA&E facilities will be conducted no later than 180 days from date of the initial inspection IAW AR 190-13.

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

3-1. Arms Room Standing Operating Procedures (SOP). CDRs, 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 include:

- a. Current CDR/DIR/FM signature.
- b. Duties for:
 - (1) Primary and alternate armorers.
 - (2) Unit AROs, and Arms Room Key and Lock Custodians.
 - (3) 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 this regulation.
- f. Reporting procedures of actual, suspected or recovered AA&E, and sensitive items losses. The Provost Marshal Office (PMO) must be immediately notified upon discovery of any loss.
- 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 (IDS) 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., FL Form 2488-E, Weapons, Ammunition, Sensitive Items, and Key Count/Inventory; Request for IDS PIC, FL Form 975-E, DA Form 3749, MAL, etc.).

3-2. Arms Room Bi-Lateral/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, conducting inventories and reconciliations.
- d. Reporting procedures for loss/stolen equipment and sensitive items IAW AR 190-45.

- 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. DPW will be contacted to correct/ensure proper illumination.

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 padlocks. Facilities not manned 24 hours a day, rifle racks 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, i.e., Type 1, Grade C, Class 4, NSN 4010-0-149-5583.

3-5. Use of Digital Arms Room Systems. The use of digital arms room for receipt, storage, issue, and accountability for unit arms room equipment is authorized IAW ALARACT 270-2011. Units and organizations are not authorized direct procurement of digital arms room Automatic Identification Technology (AIT) products without prior coordination with the Program Manager of the Joint AIT. <http://www.pdamis.army.mil/>.

a. Conventional unit CDR/DIR/FM will conduct monthly 100% hands on physical inventory and verify manufacturer serial numbers IAW AR 710-2, and AR 190-11.

b. United States Army Reserve, USA National Guard, Army Materiel Command (AMC), and Research and Development Facility CDRs/DIRs/FMs will conduct:

(1) Semi-annual 100% inventories and verify manufacturer serial numbers IAW AR 710-2, and AR 190-11.

(2) Monthly sensitive items inventories using a current Global Combat Support System (GCSS) hand receipt or the digital arms room system print out may be used to conduct monthly sensitive items inventory along with a 100% hands on physical inventory regardless of the MAL in the system reconciled and verified to match the current GCSS hand receipt.

c. Headquarters Department of Army (HQDA) authorizes physical or electronic signatures on unit arms room forms for the receipt, storage, and issue of weapons when using a digital arms room system with digital signature or Public Key Infrastructure (PKI) capability.

(1) Units will only use physical "ink" signatures when digital signatures or PKI is unavailable.

(2) The use of DA Form 3749 is not required when digital signatures or PKI capabilities are utilized in conjunction with a digital arms room system. Units are required to maintain hard copies of forms when using a system that maintains electronic copies of those forms with digital/PKI signatures.

3-6. Security of Armorer Tools. Armorer tools stored inside an arms room will be secured in locked containers using DoD approved padlocks. Hammers, crow bars, bolt cutters, and other large tools will never be left unsecured at any time.

3-7. Contract Guard Weapons. IAW AR 190-11, contract guard AA&E not U.S. Government property IAW 190-11 is the responsibility of the contractor, unless stated elsewhere in the relevant contract. Contract guard AA&E authorized for storage in military arms rooms will be accounted for and secured like military AA&E, unless otherwise specified in the written contract. These weapons and ammunition are not authorized to be stored in AA&E storage facilities containing government weapons and ammunition.

3-8. Foreign Weapons. Fully functional foreign weapons and AA&E for intelligence, research, development, test, evaluation, and training purposes will be accounted for, inventoried, and stored like military AA&E.

a. Prior registration with the Installation Property Book Office (IPPBO)/DIR of Property Book Office (DPBO) is required.

b. Units/activities are required to have functioning/non-functioning AA&E permanently listed on the unit's PBO sensitive items hand receipt, to include war trophies IAW AR 870-20.

c. Units/activities will not permanently list AA&E on their unit PBO hand receipts if they have been temporarily hand receipted for, from the Airborne Special Operations, US Army Special Operations Command (USASOC) or 82nd Airborne Division Museum.

3-9. Arming of Unit Armorers. Depending on the local threat, environment, and location of unit arms rooms or other arms storage facilities, commanders concerned will determine the need to arm unit armorers or other on-duty personnel during the performance of their duties to prevent the possible armed robbery or forcible theft of weapons and ammunition. If such personnel are armed, provisions of IAW AR 190-11 and AR 190-14 apply. Duty armorers/Guards will be qualified and armed with their assigned weapon and like ammunition under higher FPCON Charlie and Delta.

3-10. 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 dollar items) in an arms room equipped with ICIDS.

b. In such cases non-AA&E items will be accounted for and secured in the same manner as military AA&E and will be accounted for on FL Form 2488-E 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 identified number plates tending to become separated from devices will be permanently affixed by an alternate means, (i.e., engraving, permanent stamping, etc.).

d. Night vision devices, lasers, and optics will be secured and accounted for like military weapons and included in sensitive items reporting during field exercises.

e. While in garrison all categories of NVDs will be stored in the following manner:

(1) In an active arms room equipped with ICIDS.

(2) In a secured (locked) metal container with approved locks. Containers weighting less than 500 pounds will be secured to the structure (same requirements as weapons racks).

(3) Authorized Personnel. Only those personnel listed on the arms room unaccompanied access roster are authorized to access the arms room and conduct the visual count.

(4) Actions upon first accessing arms room:

(a) 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.

(b) 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 5-6c of this regulation.

(c) Results of the visual count will be recorded on FL Form 2488-E, Weapons, Ammunition, Sensitive Items, and Key Count/Inventory sheet and retained on file for 90 days.

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

(6) NVD inventories will be included in the monthly sensitive items' inventories.

(7) 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) NVDs not in possession of the assigned Soldier will be stored in a central location under constant surveillance by a guard.

(8) In Transit:

(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 on arrival.

(b) Shipping containers will be positioned so that the doors are not accessible.

(c) NVDs shipped by commercial means will be coordinated through the Readiness Business Center (RBC), Transportation Freight Office.

(d) Missing or lost NVDs will be reported IAW AR 190-45, chap 8.

(9) Waiver to policy for ICIDS requirement for NVD storage must be approved by Security Officer FORSCOM G-3/5/7 Provost Marshal/Protection (Ref message DTG 111918ZMar14):

(a) Prior to submission to US Army Forces Command (FORSCOM), a representative from IPSO will inspect the alternate NVD storage area and ensure it meets double barrier standards IAW AR 190-51. This requirement must be reflected on the waiver request. Waivers granted by FORSCOM will be reviewed annually by the requesting unit, findings will be forwarded by memo to the FORSCOM PMO for file.

(b) Waiver submissions apply only to units with insufficient storage space in arms rooms or mission requirements.

(d) Units with approved waivers found not to be in compliance during Installation Management Command (IMCOM) garrison or ACOM inspections will be required to resubmit a waiver request after correcting the deficiencies.

(e) Approval for USASOC units is the Installation Physical Security Officer. Prior to submission, a representative from IPSO will inspect the alternate NVD storage area and ensure it meets double barrier standards IAW AR 190-51. This requirement must be reflected on the waiver request, those granted will be reviewed annually by the IPSO.

3-11. Privately Owned Weapons (POWs).

a. Personnel residing on Fort Liberty will register their POWs at the All American Visitor Center.

b. Commanders will:

(1) Account for and inventory POWs, ammunition, and war trophies secured in unit arms rooms, both on FL Form 2488-E 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 FL Reg 190-11-1, and AR 190 – 11, AR 190 – 13, AR 870-20 and this regulation to ensure proper storage and control of POWs, ammunition, and war trophies.

(5) Process unauthorized AA&E IAW AR 195–5, chap 2.

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

c. No POW will be carried or transported to field training exercises or unit deployments.

Chapter 4

Administrative Requirements

4-1. Personnel Reliability Screening and Evaluation (DA Form 7708). The Screening and Evaluation will be:

a. Completed prior to assignment of a person to perform a certain duty assignment or gain access to certain materials to determine the suitability. Examples of duty assignments include, but are not limited to physical security inspectors, DA Civilian police, Security Guards, as a Unit Armorer, Key and Lock Custodian, or those involved in the control, issue, and receipt of AA&E. Examples of access to certain materials include, but are not limited to, unaccompanied access to AA&E, and controlled medical substances. For submission of a Police Records Check email the document to Police Services at usarmy.Liberty.imcom-atlantic.mbx.police-services@mail.mil.

b. Maintained on file in the area identified requiring duty/access as long as the person is authorized those duties. Personnel will be re-screened annually.

c. Re-accomplishment of the DA Form 7708 from previous CDRs/FMs is not required as long as information remains current and is not older than three (3) years. In-coming CDRs/FMs are required to review all personnel previously approved by outgoing CDRs/FMs.

d. The DA Form 7708 replaces the DA Form 7281 effective on 27 July 2019.

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

a. Current property book sensitive items listing will be used to conduct monthly weapons/sensitive items inventories IAW AR 190-11. Physical Security will inspect the last 90-120 and/or the tenure of current armorer.

b. Personnel designated by the CDR (officer, corporal and above, 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 (6) months.

4-3. Weapons and Sensitive Items Register. Arms rooms first accessed for the day require the armorer to complete a daily count and record the results on Fort Liberty Form 2488-E. If the closing armorer will not open the next day, then a joint inventory must be accomplished between the primary and alternate armorer. If this cannot be conducted the two-person rule must be followed.

a. Fort Liberty Form 2488-E, Weapons, Ammunition, Sensitive Items and Key Count Inventory Register will be used to; record daily visual count of all AA&E/sensitive items upon first access of arms room and during joint change of custody between armorers, or witness.

b. Commanders and armorers must conduct a joint inventory prior to storing AA&E and applying protective seals to the locked container.

c. Record inventory on a memorandum signed by both parties which lists contents by type, nomenclature, quantity, serial number if applicable, annotate the protective seal number used and post a copy of the memo on the exterior of the locked/sealed container. 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. An entry in the remarks section of Fort Liberty Form 2488-E and PBO inventory will reflect the property as "validated by protective seal #_____".

d. Personnel completing Fort Liberty Form 2488-E will:

(1) Compare the last inventory from the previous day with the first inventory of the present day, any differences will be reported immediately. Should discrepancies be noted, a joint inventory will be conducted by the individual opening the facility and an officer/NCO designated by the CDR to witness the inventory, line through block 6 of Fort Liberty Form 2488-E, print "Witness" and sign. Conduct a joint inventory as required if a change of custody of the AA&E/sensitive item storage container keys occurs.

(2) Ensure individuals accept responsibility for the arms room and contents by printing their name and their signature in the "Signature of Accepted Individuals" block 7 of Fort Liberty Form 2488-E.

(3) 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.

(4) Ensure the Total block indicates the total quantity of AA&E/sensitive items authorized by the Modified Table of Organization and Equipment (MTOE). The "In Arms Room" block and "Signed Out" block must add up to the "Total" block. (The total amount will be the same as listed in the PBO Sensitive Item listing).

(5) Maintain a properly completed Fort Liberty Form 2488-E on file for 90 days.

(6) Once deployed property has been deleted from the rear detachment hand receipt, the armorer can drop the count (deployed property) from the FL Form 2488-E. (An entry in the remarks block is required.) Example of FL Form 2488-E (Nomenclature block)
Type M4 RD M4 DEP M68 RD M68 DEP.

In arms room	10	120	0	120
Signed out	0	0	0	0
Total	10	120	0	120

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 Soldiers:

(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 where it is visible to the public.

4-5. Department of the Army Equipment Receipt (DA Form 3749).

a. When a single item (weapon or sensitive item) is needed for issue to more than one (1) individual, the armorer will prepare DA Form 3749 for each authorized item. Unit of issue will be IAW DA Pam 710- 2-1, para 5-6d (1) through (4), except that control sheet (MAL) 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, regardless of time frame requires the turn-in of a DA Form 3749 (primary) and DA Form 2062 or a weapons control log entry (secondary), 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.

(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, Fort Liberty Form 2488-1E will be used in conjunction with 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.

c. Account for weapons/sensitive items on Fort Liberty Form 2488-1E laterally transferred or forward deployed until they have been reconciled and a new hand receipt has been issued by the PBO.

d. Deployments. A Fort Liberty Form 2488-1E will be used and maintained by units during deployments:

(1) Maintain the original form listing weapons/sensitive items issues in the arms room.

(2) A copy of Fort Liberty Form 2488-1E should be taken with deploying units.

(3) Originals will be maintained on file at the unit's rear detachment until the unit redeploys.

e. Digital issue/turn-in procedures for weapons are not authorized. The Soldier will enter, in ink, the nomenclature and SN of the item received, the time of issue, and his or her signature as it appears on DA Form 3749. When weapons are turned in, close out the control sheet, return the Soldier's DA Form 3749. The person receiving the weapon will enter the date, time, and his or her initials on the control sheet (per DA Pam 710-2-1. The same process will be used for equipment other than weapons (i.e., other weapon items/components stored in an arms room).

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

a. Only DoD approved padlocks will be used to secure AA&E racks/containers.

b. The S&G 951 high security padlock is the only authorized lock for securing entrance doors to AA&E facilities.

(1) Arms vaults with combination locks that protect weapons and ammunition must meet the requirements of Federal specification FF-L-2937, Combination Locks, Mechanical for new containers.

(2) Existing weapons and ammunition containers may continue to use combination locks that meet the requirements of Underwriters Laboratories Inc. (UL) Standard 768, Group 1.

(3) Digital combination locks are not recommended for use on AA&E vaults. For information/ordering, refer to the DoD Lock Program at the below web address: Link for new S&G 951 (key operated): https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock/SecurityHardware/CombinationLocks.html.

c. Use 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 (1) year.

(5) Ensure SDNCO logs all issues and returns of AA&E key containers on DA Form 1594, Staff Duty Journal and maintain on file for a minimum of 90 days.

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) Two-person control rule is required for access to AA&E keys. Key container(s) will be stored with SDNCO and the key that opens the container must be controlled by the unit AA&E Key and Lock Custodian.

(2) Armorers will contact the AA&E Key Custodian for access to the key that unlocks the key container.

(3) Primary and alternate sets of keys will be maintained in separately locked containers or in a sealed envelope with controlled access; alternate set of keys will be maintained by the S2.

(a) Primary arms room keys will be placed in a locked metal container and secured with a DoD approved padlock at the end of each duty day when not in use. The locked container will be logged in/out to the BDE/BN SDO/SDNCO on DA Form 1594 and not on DA Form 5513; units without a Staff Duty will be required to maintain primary keys in a GSA approved safe with controlled access.

(b) 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.

(c) Keys and containers will not be stored in the same container with classified material; however, segregation in individual drawers is acceptable. Containers are not required to meet the 500-pound rule as long as the container/safe is located in a secure room or under continuous surveillance. Arms room/storage area keys will not be removed from the BDE/BN/CO area.

(d) The transfer of arms room keys between armorers will be recorded on the FL Form 2488-E during joint change of custody inventories.

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

(f) Use of master/keyed alike locks is prohibited.

(g) Combination padlocks are prohibited.

f. Arms Room Key and Lock Custodian will ensure:

(1) A favorable Personnel Reliability Screening and Evaluation (DA Form 7708) and AROC has been completed, and a copy of each 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) Primary arms room keys are issued to the primary armorer on a DA Form 5513 for a one-time initial issue. Note: If the armorer is going on leave, temporary duty, etc., for longer than 30 days, the Key and Lock Custodian will have the alternate armorer sign one (1) time for the arms room keys.

(7) Issuance of the alternate set of arms room keys (one (1) 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) to the next higher S2 on DA Form 5513 (one (1) 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. Note: Escape keys will not be included in the arms room key control system.

g. Lost or Stolen Keys and Locks. When keys to a lock to secure AA&E are missing or stolen, the Military Police (MP) will be notified, and a police report completed immediately. The affected lock will be immediately 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. Keys and combinations to locks for AA&E storage facilities, arms racks, IDSs (operational or maintenance), or key containers will not be removed from the installation, except to provide for protected storage elsewhere (i.e., deployment, off installation unit movement, etc.) IAW AR 190-11, chap 3.

4-8. Standard Form (SF) 700, Security Container Information Sheet. An 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 (4) 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 with S2.
- 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 an SF-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. A SF-702 are not required for separate NVDs, ALSE storage facilities; however, a SF-701, Activity Security Checklist is required.
- 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 AR 190-11, app G, and require a DA Form 4604-R, Security Construction Statement.
- b. A Security Construction Statement will be issued by a qualified Directorate of Public Works (DPW) Engineer (910) 396-0321 every five (5) 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.

4-11. Required Signage.

- a. Local and North Carolina 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. Reference UNCLAS ALARACT 131/2003, Subject: HQDA Message 151100ZJAN98, Subject HQDA Message in Interim implementation of the Lautenberg Amendment. This amendment makes it unlawful for any person to transfer, issue, sell or otherwise dispose of firearms and ammunition to any person whom he or she knows or reasonably believe has been convicted of a misdemeanor crime of domestic violence.

(1) A copy of the Lautenberg Amendment Message as contained in Headquarters Department of the Army (HQDA) UNCLAS ALARACT 131/2003. This will be posted on the exterior wall adjacent to the arms room entrance door.

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 (3) 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 and posted/protected from public view inside the arms room or AA&E facility.

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

c. Escorted persons will not be left unsupervised in the arms room at any time.

4-13. Physical Security and Crime Prevention Officer's Course, and Arms Room Operators Course.

a. Physical Security Crime Prevention Officers Course (PSCPOC).

(1) Attendance is mandatory for BDE/GRP/BN/SQDN/Co level and DIR PSOs, and S2s. The course is designed to provide PSOs with assistance in developing and maintaining an effective Physical Security program.

(2) A PSO and CPO will be appointed in writing: At BDE/GRP levels a MSG/E-8 or MAJ/O-4 or above; at DIR/FM levels a GS-9 or above; at BN/SQDN levels a SFC/E-7 or CPT/O-3 or above; and at CO/TRP/ BTRY levels a SSG/E-6 or LT/O-1/2 or above as the unit PSO/CPO.

(3) PSCPOs are required to attend PSCPOC training with the IPSO within six (6) months of duty appointment. A sample appointment order is provided, see app V.

(4) Course is conducted once per quarter.

(5) Course hours: 0900-1200.

b. Arms Room Operations Course (AROC).

(1) Attendance is mandatory for Officers in Charge (OIC), Noncommissioned Officers in Charge (NCOICs), armorers, S2s, command/unit PSOs and AA&E key custodians, and highly recommended for CDRs/1SGs. The course is designed to provide personnel responsible for AA&E and arms rooms with an overview and familiarization of arms room operations.

(2) Course is conducted twice on the first Wednesday of each month.

(3) Course hours: 0900-1200 and 1300-1500.

c. General Information. The PSCPOC is held in the DES classroom, building 2-5935 and a seat reservation is required. AROC attendance is a "first come, first serve" basis and the location varies based on availability (phone physical security office for location). S2s/Security Managers/PSOs may request unit classes for 20 or more individuals by contacting the IPSO at (910) 396-9109/1962.

Chapter 5 Administrative Key and Lock Control 5-

1. Key and Lock Custodians.

Key control and accountability must be established at all functional levels IAW AR 190-51. The CDR will appoint a primary and alternate Key and Lock Custodian in writing. Primary custodians are authorized to approve and sign key depository access rosters. Access rosters will be posted on the exterior of all key depositories. Appointment orders will not be used in lieu of access rosters.

a. Units with multiple key depositories which are located side by side require only one (1) 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."

b. Master keys/keyed alike set locks are not authorized unless the unit has a HQDA waiver. Exceptions are:

(1) Facilities with multiple doors that open one (1) or all doors leading to the same interior.

(2) Keyed-alike and master-keyed locksets will not be used for multiple vehicles but can be used for a single vehicle and its compartments. See AR 190-51, app D prior to use.

(3) Storage containers with multiple doors where opening one (1) door leads to the same interior of the container. Other areas contained within are not authorized this exception.

c. Keys and locks used to secure government equipment will be included in a key control system.

d. 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.

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.

b. Newly appointed Key and Lock Custodians will conduct an initial 100% key/lock by serial number, and semi-annual inventories thereafter, IAW AR 190-51. Inventories will be recorded on page 2 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 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 (2) 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 a listing of low security padlocks see below:

KA - Keyed Alike/KI - Keyed Individually/CID-Commercial Item Description

NSN DESCRIPTION: 5340-00-158-3805 Padlock (without chain): Steel case and shackle.
5340-00-158-3807 Padlock (with chain): Steel case and shackle.
5340-01-437-0625 Steel case 1 3/4" body width. Set: 6 Locks.
5340-01-588-1916 Padlock (with chain): Steel case and shackle.

Note: List is not all inclusive, most common DOD approved locks are manufactured by "American Lock TM", "Master", and "Federal". 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. If a key to a padlock is lost/missing, an inquiry will be conducted and documented. The padlock will be replaced and recorded 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 chain of at least 1/4 inch in thickness.

f. Electronic locks and locking systems may be used unless specifically prohibited, and IAW AR 190-51 have the following minimum design criteria:

(1) Be compliant with Federal Information Processing Standard.

(2) Have back-up battery power of at least 4 hours.

(3) Be placed in the fail-secure mode.

(4) Have appropriate life-safety hardware.

(5) Have a mechanical key override.

(6) Have serial-numbered key devices accounted for on a DA Form 5513 or an electronic form containing equivalent information.

(7) Have a 1-inch throw deadbolt, or mortise lock if the standards above cannot be met.

g. AR 735-5 will be followed for guidance concerning financial liability for the loss of a key due to negligence or willful misconduct.

5-5. Electronic Card Access Accountability.

a. Access card control and accountability must be established at all functional levels IAW this regulation. The CDR 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.

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.

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

c. 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 (1). Cards cannot be engraved but can be written on with a permanent marker.

d. The Access Control Administrator shall issue a master access card to the designated Staff Duty or Charge of Quarters (CQ) utilizing a DA Form 2062 or Staff Duty Journal.

e. System master access cards will be maintained and always secured. 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 2062 and will be secured in a staff duty safe. 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).

f. 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 Logbook 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) Seals will be inventoried monthly (using modified DA Form 5513 or the equivalent).

c. Table of Approved Seals for AA&E Shipments. The following seals are required for the protection of AA&E and classified shipments.

Description	National Stock Number
Cable Seal Lock	NSN 5340-00-084-1570
Cable Seal Lock	NSN 5340-01-177-7405
Bolt Seal	NSN 5340-01-237-7646
Car Ball Seal	NSN 5340-01-237-7646

*Information can be obtained by contacting the Defense Logistics Agency (DLA) at: 1-877-352-2255, DSN: 661-7766, Commercial: 269-961-7766, or http://www.dlis.dla.mil/webflis/pub/pub_search.aspx

Chapter 6

Integrated Commercial Intrusion Detection System (ICIDS)

6-1. Intrusion Detection System (IDS) Alarms. All unit arms rooms and vaults will be protected by a minimum of two (2) types of alarm sensors (balance magnetic and volumetric sensor such as passive infrared).

- a. Facilities without an operational IDS will be protected with armed guards 24 hours a day IAW para 6-6.
- b. The ICIDS is the only Army approved alarm system for AA&E/communications security (COMSEC) facilities on Fort Liberty.

6-2. Alarm Activations.

- a. Integrated Incident Management Center (I2MC) 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 I2MC, (910) 396-3071). Authorized personnel must reset the alarm immediately if no violations are found.
- d. The I2MC alarm 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 an ICIDS Alarm Test Record for 90 days.
- b. To conduct a test, the primary or alternate armorer must provide the I2MC, (910) 396-3071 with their name, building, and zone number.
- c. The unit armorer will take all directions from an alarm monitor in order to facilitate and complete the alarm test.

6-4. Personal Identification Code (PIC). A current, accurate, IDS PIC Request Form (DES IDS PIC Form JUN 2023) digitally signed by the CDR/FM is required to obtain a PIC for an ICIDS alarmed area.

- a. PICs will:

Be issued to personnel requiring unaccompanied access to an ICIDS alarmed area or facility.

(1) Not be shared with other personnel.

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

b. Each CDR/DIR/FM must immediately notify the Physical Security 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 DES, Physical Security Office.

d. PIC Request Form can be downloaded at: [FL 975 June 2023.pdf \(army.mil\)](#)

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 I2MC and the Chain of Command (COC).

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

c. Immediately notify the PMO at (910) 396-0391 and the Physical Security Office at (910) 396-9109.

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

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

6-6. Intrusion Detection System Failure Procedures.

a. In event of an AA&E IDS failure, the unit/activity will immediately post guards armed with live ammunition for the weapon for which they are assigned and qualified IAW unit SOPs. All guard personnel will be briefed on the Use of Deadly Force, IAW AR 190-14.

b. Security Checks. For extended IDS failures designated personnel (e.g., SDNCO/guard personnel) are required to conduct security checks of IDS protected AA&E facilities during non-duty hours on an irregular basis to not establish a pattern. Checks will be recorded on a SF-702 or DA Form 1594, Daily Staff Journal. Records of security checks will be retained in unit files for a minimum of 90 days.

6-7. Intrusion Detection System Work Orders.

a. Units/activities must report problems and malfunctions of IDS sensors or systems to the I2MC at (910) 396-3071. The I2MC 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 the Physical Security ICIDS Office and completed based on workload and priorities:

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

c. Work Order Priorities are as follows:

(1) Sensitive Compartmented Information Facility (SCIF).

(2) High Risk Target (HRT).

(3) AA&E.

Communication Security.

(4) All others.

d. The I2MC will direct units without operational ICIDS to comply with IDS failure procedures in para 6-6a, and IDS work order procedures in para 6-7a.

e. Individuals with authorized access to the affected area must be on standby during normal duty hours 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. Post armed guards at motor pools IAW FPCON levels.

b. Develop SOPs for motor pool guards.

c. Establish guard procedures during operational hours:

(1) Control gate egress and regress at all times through the use of DA Form 1594.

(2) Check all incoming/outgoing vehicles for a valid dispatch and equipment to deter and protect motor pool from pilferage, theft, and unauthorized removal of equipment and materiel.

(3) Prohibit entry of all POVs into motor pools. Only exception will be for units engaged in deployment exercises IAW unit SOP and AR 190-51.

(4) Check all vehicle operators for valid identification (ID), (e.g., common access cards (CAC) for military, DoD employees or contractors, valid state driver's license, and operator's license (OF Form 346, US Government Motor Vehicle Operator's ID Card).

(5) Verify motor pool access of non-military personnel against organization access rosters. If unavailable to verify access, the guard will contact the SDO, NCOIC, Motor Pool OIC, unit S2 or PSO. Guards will follow incident reporting procedures IAW unit/organizational SOPs.

d. Motor pools will be properly secured during non-operational hours. Security checks will be conducted IAW AR 190-51 and or FPCON increased requirements.

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 motor pools to the maximum extent practicable (AR 190-51, para 3-11). Exceptions include deployments, ranges, training areas, or when authorized to park at rail shipping yards, or airfields. It is recommended that commanders secure NTVs in unit motor pools when not in use.

c. IAW AR 190-51 tactical vehicles will be rendered inaccessible, locking 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.
- f. "No POV" signs will be posted by all motor pool entrances.
- g. Tactical vehicle parking areas will be at a distance from the perimeter fence as determined by the risk analysis. A risk level II requires 20 feet stand-off or as far as possible.
- h. Unit security guard checks will be determined by the risk level.
- i. Security measures for General Services Administration vehicles and U.S. Army Corps of Engineers-owned vehicles, boats, watercraft, and equipment are covered in AR 190-51 (para 6-24).

7-3. Perimeter Fencing and Lighting.

- a. Perimeter fence. Fencing will meet the requirements of US Army Corps of Engineers
- b. Drawing Code STD 872-90-00 Series. The minimum height for new fencing will be seven (7) feet tall not including the top guard. Fencing will be at least nine (9) gauged and the bottom of the fence will not be above two (2) inches off the ground. For fencing requirements refer to AR 190-51 and ATTP 3- 39.32.
- c. Perimeter wall. Any wall over six (6) feet tall which delineates a boundary and serves as a portion of the perimeter fence. These walls may be constructed of reinforced concrete, masonry, or stone.
- d. Lighting. Vehicle parking areas, except those for empty trailers, will be lighted during the hours of darkness. Storage areas will be always provided with operational interior/exterior lighting during the hours of darkness. Physical Security Officers 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.
- b. Use of master keys or lock sets to secure vehicle steering wheels is prohibited.
- c. Consolidated motor pools will designate one (1) 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/Tools. Commanders 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.

- a. Access rosters must be posted by the entrance to storage locations.
- b. "Off Limits to Unauthorized Personnel" signs will be posted at entrances.
- c. Storage areas will meet the security requirements of Risk Level I IAW AR 190-51, app B. Caging material is only authorized if it completely encloses the room. Tool containers loaded on military vehicles will be secured when not in use.
- d. Locks will be DoD approved.

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

- e. Mechanics will sign for their tool kits/box and will personally retain their key. A copy of the key will be retained by their supervisor or CDR and will be stored in a locked container with controlled access.
- f. Standard Operating Procedures will address issues, receiving procedures and end of duty day reconciliations.
- g. Tool kits and boxes will be secured when not in use.
- h. Requirements for manned and unmanned aircraft systems, hand tools, tool sets and kits, and shop equipment see AR 190-51, AR 710-2, AR 735-5, and DA Pam 710-2-1.

7-6. Repair Parts not at Installation Level Supply Support Activities and Direct Support Units With an Authorized Stockage List (ASL).

- a. Unit and activity repair parts will be stored in a single area, readily accessible to only designated maintenance or supply personnel.
- b. Access rosters must be posted by entrances to storage locations.
- c. "Off Limits to Unauthorized Personnel" signs will be posted at entrances.
- d. Locks will be DoD approved IAW AR190-51, app D.
- e. Local sign out procedures will be established for accountability of repair parts.

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, while on Fort Liberty will report their loss or theft immediately to the Fort Liberty MP, (910) 396-0391/2. A SIR must be completed and submitted IAW AR 190-45, chap 9 and this regulation.
- 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.

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. Immediately notify the COC upon discovering lost or stolen sensitive item.
- b. Notify the Fort Liberty MP at (910) 396-1179 within two (2) hours of discovery.
- c. Notify the Fort Liberty Operations Center (FLOC) by telephone within a reasonable time frame of discovery and submit written report of incident to the FLOC within 24 hours. FLOC contact number is (910) 396-0371.
- d. Immediately cordon off the scene of the lost or stolen item and assemble all personnel who had possible access to, or responsibility for the missing item.

Form a search party. The size of the search party is determined by the unit CDR and/or the COC. At a minimum, the areas searched should include the area from where the weapon or sensitive item was discovered lost or stolen to the last place it was accounted for.

e. Initiate a detailed search, to include a complete inventory of weapons and other sensitive item. Seek advice from the servicing Staff Judge Advocate (SJA) before inspecting personal areas or equipment. Segregate personnel who may have knowledge of the loss or theft and make these personnel available to the Criminal Investigative Division (CID) or investigating officials.

f. Notify adjacent units regarding the incident to ensure they are aware of the incident and have not located the lost or stolen item.

g. Maintain unit in the field/location of the loss or theft until the weapon or sensitive item is found or a release from the search is received by the unit's senior command (i.e., higher Headquarters).

h. The Incident CDR retains approving authority for granting an amnesty period. However, Incident CDRs must consult the Staff Judge Advocate (SJA) office prior to granting an amnesty period.

i. 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 (ANCDs)/Signal Operating Instructions (SOI).

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

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

Chapter 9 Crime Prevention

9-1. Responsibilities.

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

(1) Establish a CP Program and monitor its effectiveness. Crime Prevention programs will be inspected by Installation Physical Security every 18 months.

(2) Appoint in writing: At BDE/GRP levels an MSG/E-8 or MAJ/O-4 or above; at DIR/FM levels a GS- 9 or above; at BN/SQDN levels a SFC/E-7 or CPT/O-3 or above; and at CO/TRP/ BTRY a SSG/E-6 or LT/O-1/2 or above as the unit CPO. Crime Prevention Officers are required to attend PSCPOC training with the IPSO within six (6) months of duty appointment. A sample appointment order is provided, see app V.

(3) Establish a CP SOP IAW app E. This chap, although not all-inclusive will, serve to develop a unit's CP SOP. Battalion/SQDN/Co. level CP SOPs will complement higher headquarters CP SOPs. SOPs will include responsibilities for CQ to:

Conduct security checks a minimum of two (2) 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 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).

- (a) Comply with fire and safety requirements.
- (b) Secure all doors except the main entrance doors after duty hours and ensure exits provide required safety but deny entry.
- (c) Properly secure any unsecure property and annotate those actions in the Staff Duty Journal.
- (d) Report all incidents or suspected incidents to the CoC and to the Installation Provost Marshal Office IAW AR 190-45.
- (e) Immediately report observed criminal acts or suspicious activity to the Fort Liberty MP Station, chain of command, and document such reports on the Staff Duty Journal.
- (f) Ensure building doors and windows are adequately secured.
- (g) Ensure CQ/SDO/SDNCO (lowest level physically manned) duty logbooks contain a current billeting roster of personnel with their assigned rooms.
- (h) Control visitor access to unit and billeting areas.
- (i) Prohibit access to minors/juveniles, 17 years old and younger, who are not US Military personnel, unless accompanied by parent or legal guardian.
- (j) Deny access to personnel who have been identified by the CoC as prohibited entry into the billets.
- (k) Prohibit vendors and solicitors' access without prior written approval by the CoC.
- (l) Crime Prevention Officers must conduct announced and unannounced and quarterly CP inspections and assessments of headquarters and subordinate CP programs. Crime Prevention Officers must maintain results on file for 12 months.
- (m) Crime Prevention Officers must ensure newly assigned personnel receive and acknowledge the unit CP in-brief (app E) 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.
- (n) Crime Prevention Officers must schedule and conduct semi-annual CP training. Files will be maintained for 12 months.
- (o) 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.
- (p) Crime Prevention Officers must ensure secure storage areas are available to store a Soldier's personal property and organization clothing and individual equipment (OCIE). If adequate space is not provided Garrison will be contacted for providing acceptable alternatives.
- (q) 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 FL Form 4986, Personal Property Record when

inventorying or declining to inventory their property. Completed and signed FL Forms 4986 will be maintained and updated regularly by the CPO and the Soldier's First Sergeant. The Soldier's copy must be always secured in an inconspicuous area.

(r) 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 CoC.
- (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) Mark all personal property.
- (7) Mark property with "USA", and with a personally identifiable number (i.e., unit SOP, last four numbers of Soldier's social security number, license number, etc.).
- (8) Not leave valuables and money in pillows, mattresses, or in unsecured nightstands, desks, or lockers.
- (9) MTOE/OCIE will not be stored in personally owned vehicles (POVs) or military vehicles, on or off post for any reason. Per AR 190-51, 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, footlocker, 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. Keys to access separately locked rooms will be placed in the unit key depository and controlled by the unit Key and Lock Custodian.
 - (c) Marking of government property shall comply with AR 190-51, app C.

c. Unit Supply will:

- (1) Establish and follow requirements for the accountability, control, security, and handling of bolt cutters as AR 190-51, app D. The purpose of this control is to increase key accountability, contain costs incurred by replacing cut padlocks, and incidences of unauthorized removal of equipment. Note: Primary and alternate key control personnel are the only personnel authorized to be issued the bolt cutters. When issued, supply personnel will notate in the logbook the date of issue, name of recipient, purpose for issue

(exact location of lock to be cut), and the initials of the supply person who is issuing the bolt cutters. Supply personnel will then have the key control custodian sign for the bolt cutters using DA Form 3161 (Request for Issue or Turn-In) or DA Form 2062 (Hand Receipt/Annex Number). Bolt cutters will be signed back into the supply room prior to the end of the day they were signed out. 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 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. 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.

9-2. Health and Welfare Inspections.

a. It is recommended that CDRs consult their servicing SJA before conducting health and welfare inspections.

b. Commanders will notify the Fort Liberty MP of any prohibited/suspected item(s) found.

c. Confiscated items will be maintained by the CoC until disposition. Illegal items will be released to Fort Liberty MP as appropriate.

d. Commanders may request PMO (K-9/Narcotics Team) assistance during Health and Welfare inspections.

9-3. 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 perimeter doors to the billets.

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. Per DA Pam 710-2-1, Dayroom televisions/DVD players and other high dollar government property will be sub-hand receipted to the Barracks or Supply NCOs. Per AR 190-13, the property should be properly secured and inventoried for proper accountability.

g. Privately owned weapons are prohibited in the barracks. Refer to FL Reg 190-11-1, chap 9 for a complete listing of prohibited weapons.

h. Commanders and directors will develop physical security plans for barracks to the extent possible. At a minimum addressing the requirements in AR 190-13, app D, will be reviewed annually, revised as

needed to remain current. A brief statement affirming currency will be placed on the front page in this format: Certified current by (commander, director, or designated representative) (date). The plan is an inspectable item and will be included in command operations inspections, installation inspections, and similar inspections and assessments. Note: The plan does not have to be a separate document, it can be an annex to a barracks management plan, a protection plan or similar encompassing plan, but will address each planning element identified in the app.

9-4. 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. DPW will prioritize lighting issues identified in para 9-4a.

9-5. 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, app D.
- b. Commanders will coordinate with FLs Army Field Support Brigade (AFSBN) for use of the installation POV storage facility during deployment for storage of POVs, all-terrain vehicles, boats, recreation vehicles, etc. Commanders will establish unit SOPs to secure and provide access control to designated storage areas if the installation POV storage facility is unavailable. All designated POV storage areas will be fenced and adequately lighted.

Chapter 10

Installation Access Control Procedures

10-1. Policy. Security personnel will verify the ID of all persons entering Fort Liberty through the installation's visitor centers and vehicle access control points (ACPs) IAW Fort Liberty Memorandum 190-13.

10-2. Procedures.

a. Screening Personnel Records:

(1) A check of records through the National Crime Information Center (NCIC) Interstate ID Index (III) is the Army minimum baseline background check for entrance onto Army installations for non-CAC holders and visitors.

(2) Authorized credentials for DoD installation access and Automated Installation Entry (AIE) pass and cards are contained in Fort Liberty Memo 190-13.

(3) ACP and Visitor Control Center locations and hours of operation and application for Fort Liberty Installation access cards (Appendix N DES Form 118) can be found at the following web site: <https://home.army.mil/Liberty/index.php/my-fort-Liberty/all-services/gate-information>.

b. ID Requirements:

(1) All persons aged 18 and over must present photographic (photo) ID for access to Fort Liberty IAW AR 190-13, chap 8-8.

Persons below the age of 18 are not required to present photo ID unless operating a motor vehicle. However, will be vouched for by an individual cleared to enter the installation IAW AR 190-13, para 8-8 (this may be suspended).

(2) Persons aged 16 and older operating a motor vehicle must present a valid driver's license (DL), vehicle registration and proof of insurance for the vehicle which they are operating.

c. Identification Documents. Persons in possession of the following IDs are authorized unescorted access onto Fort Liberty:

(1) Department of Defense Common Access Card. Per DoDI 8190.3, the DoD CAC is the standard ID card for Active and Reserve uniformed personnel, DoD Civilian employees, eligible contractors, and some designated foreign nationals. The DoD CAC shall be the principal access control card which enables access to buildings, facilities, installations, and some limited controlled spaces.

(2) Department of Defense (DD) Form 2 and DD 1173. The Uniformed Services ID and Privileges Card, (DD Form 2 and DD Form 1173) are issued to military dependents and retirees.

(3) Automated Installation Entry Pass or Card. The pass or card provides a means to effectively screen a population that does not necessarily have DoD affiliation (i.e., visitors, contractors, sub-contractors, vendors, etc.). The pass and card are an access credential issued by Fort Liberty Visitor Control Centers (VCCs) to persons who successfully pass a NCIC level III background check, and who do not otherwise meet the requirements for a CAC.

(4) Other acceptable forms of ID include:

(a) Air Force (AF) Form 354, Civilian ID card.

(b) Department of the Army Form 1602, Civilian ID card.

(c) Department of Defense Form 489, Geneva Convention ID card for Civilians.

(d) Department of Defense Form 1173, Uniformed Services Identification and Privilege Card.

(e) Department of Defense Form 1934, Geneva Convention ID card for Medical and Religious Personnel.

(f) Department of Defense Form 2574, Armed Forces Exchange Services ID, and Privilege card.

(g) Department of Defense Form 2764, US DoD/Uniformed Services Civilian Geneva Convention ID.

(h) Department of Veterans Affairs, Veteran Health Identification Card (VHIC). Veterans eligible solely under the act who are eligible to obtain a Veteran Health Identification Card will use this credential for in-person installation and privilege access. The card must display the Veteran's eligibility status (i.e., PURPLE HEART, FORMER POW or SERVICE CONNECTED). Veterans eligible solely under this act who are not enrolled in or are not eligible to enroll in VA health care, or who are enrolled in VA health care, but do not possess a Veteran Health Identification Card will not have in person access for in-person commissary, exchange, and MWR retail privileges. Upon the first visit, eligible Veterans and caregivers must stop at the visitor control center. Veterans may enroll for recurring access, which would allow them to proceed to the gate for entry upon subsequent visits without having to stop again at the visitor control center. As with all other individuals seeking access to DoD installations, all eligible Veterans must pass a basic on-the-spot background check prior to enrolling, and an automated check each time they enter the installation. Veterans with felony convictions, felony arrest warrants, or other types of derogatory information related to criminal history or terrorism will not be permitted entry. Note: The Veteran Health Identification Card (VHIC) is not to be confused with the Veteran identification card. The Veterans

Identification Card (VIC) is a form of photo ID used to get discounts offered to Veterans at many restaurants, hotels, stores, and other businesses and will not grant access.

(5) Non-DoD affiliated persons must present one (1) of the following forms of ID to request access to FL:

(a) Valid state DL or state photo ID card.

(b) Local, state, and federal agencies including members of Congress, their staff representatives and elected public officials with official photo ID cards will be granted access. Staff personnel who have felony convictions within 10 years will require a waiver to access post.

(c) Valid ID or DL from US Territories (i.e., Puerto Rico, Guam, and Virgin Islands).

(d) Valid passport from other countries cleared by the State Department.

d. Unescorted/Unimpeded Installation Access. Unescorted persons requesting access onto Fort Liberty must have a valid purpose and an authorized form of ID per para 4a thru f above. Unescorted access to Fort Liberty is normally reserved for the below listed categories, unless Random Antiterrorism Measures (RAM) or an increase of Force Protection Conditions (FPCONs) is directed:

(1) DoD ID cardholder.

(2) Persons issued an AIE visitor pass or card.

(3) Gold Star and next of kin survivor Family member(s), Survivor Access Card (DD 1173) or Civilian Identification Card with "Survivor" typed in the status block cardholders.

(4) Other federal agency personnel with an approved ID document or AIE visitor pass.

(5) Federal, state, and local government officials driving official, emergency vehicles (non-emergency capacity) or POVs must present their credentials (photo ID and DL). All federal, state, or local emergency vehicles responding to an emergency (Mutual Aid Plan) on the installation must notify I2MC or MP station operations desk. If advance notification has not been received, the I2MC or MP desk must verify the response with the appropriate emergency agency.

(6) Government (federal, state, and local) vehicles with approved dispatch/registration documents. Drivers must possess authorized photo ID documents.

(7) Pedestrians and bicyclists with an approved form of ID, (i.e., DoD ID card or AIE card or visitor pass).

(8) Verification documents do not automatically constitute unimpeded access. Pedestrians, bicyclists, and vehicle operators may be subject to screening/vehicle screening IAW installation Force Protection directives.

e. Visitor Pass:

(1) Persons operating a motor vehicle and request to apply for an AIE visitor pass must produce a valid permanent or temporary state/US Territories DL, state registration and proof of insurance for the vehicle they are operating.

(2) All others applying for an AIE visitor pass must produce a valid permanent or temporary state/US Territories ID.

(3) The Installation VCC will issue an AIE visitor pass, not to exceed one (1) year.

(4) Passes are valid until midnight of the printed pass-through date.

(5) Access control guards will examine, and scan all passes during gate operations to ensure the AIE system verifies the pass.

(6) AIE visitor passes are non-transferable.

f. Sponsorship/AIE Visitor Cards:

(1) Only DoD ID cardholders can sponsor guests, other service members, volunteers, etc, onto FL by completing DES Form 118 (Appendix N).

(2) Friends/Partners of Liberty. The Senior Commander (SC) or his designated representative can approve Friends/Partners of Liberty access cards for person(s) who require recurring access to FL for functions or official business. Access cards will be issued based on a person's needs and may be issued for a maximum of one (1) year.

(a) Friend/Partner access cards are generally reserved for community or municipal leaders requiring recurring access to installation leadership (i.e., government officials, mayors, council members, school superintendents, board presidents, community connectors, privatized military and business alliances, and city and county community partners).

(b) Persons aged 18 years and older with an AIE card are not authorized to sponsor non-DoD ID card passengers.

(3) Designated Representatives. Brigade/Group/Battalion/Squadron or higher CDRs, Executive Officers, Directors, Deputy Directors, or Contract Officer Representatives (CORs) can hand deliver or email a completed and approved DES Form 118 to the FL DES/Physical Security Division, Department of the Army Security Guards Army Security Guards (Chief of Guards), phone (910) 432-1200/1199. A VCC representative will contact and request the sponsored person(s) report to the VCC for issuance of their access card.

g. Controlled Installation Access (pass or card). Non-DoD affiliated visitors must have a valid purpose for requesting installation access and must possess an authorized form of ID per para 16-2b. Visitors will be issued an AIE pass or card at the All American VCC. Visitors must be sponsored or escorted by an authorized DoD ID cardholder.

(1) Commercial/School Bus Drivers. Drivers have the option to process for an AIE visitor pass, not to exceed one (1) year or receive sponsorship for an AIE Partner card.

(a) Sponsored drivers must submit DES Form 118 to their government sponsor for processing.

(b) Drivers must present employer (i.e., county/school district) specific photo ID card with state DL when applying for an AIE card at a VCC. Drivers may receive an AIE visitor card, not to exceed one (1) year. Note: Access control guards will conduct a walk-through of buses and conduct random spot checks of student IDs.

(2) Commercial/Delivery Trucks (i.e., 15 passenger or larger not for personnel transport, Federal Express (FedEx), United Parcel Service (UPS), U-Haul, tractor trailer, etc.):

(a) Will be directed to the Vehicle Cargo Inspection Facility (VCIF) at the Truck Plaza entrance at Knox and Cook Streets between the hours of: 0500-2100 on weekdays; and 0500-1300 on weekends to process for an AIE visitor pass. During non-operational hours of the Truck Plaza, commercial delivery drivers may access the Longstreet and Honeycutt ACP.

(b) The Longstreet and Honeycutt ACP are the alternate VCIF and remains operational 24/7.

Delivery drivers must possess a current AIE pass or card or must have planned 48 hours in advance through the Access Control Office, (910) 432-1199/1200 prior to the requested date of entry to FL.

(c) Drivers must possess a bill of lading for delivery bearing an address on the installation.

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

(e) All delivery vehicles will be subjected to a 100% vehicle inspection. Maximum utilization of available military working dog teams and explosive detection equipment will be implemented.

h. Recreational Vehicles. A Recreational Vehicle (RV) include motorhomes, campervans, caravans (also known as travel trailers and camper trailers), fifth-wheel trailers, popup campers and truck campers.

(1) RVs must enter through the Truck Plaza entrance at Knox and Cook Streets between the hours of: 0500-2100 on weekdays; and 0500-1300 on weekends to process for an AIE visitor pass. During non-operational hours of the Truck Plaza, RV(s) may access through the Longstreet and Honeycutt ACP. Note: Access control guards will conduct a walk-through of RVs.

(2) CAC Card Holders (Active Duty) and DA/DOD CAC Card Holders (Reserve and National Guard Members on active duty, Government Employees) are authorized to enter any gate at any time while operating an RV.

(3) Teslin Card Holders (Retirees and Family Members), AIE Paper Pass/Card Holders, and Contractors must use one (1) of the commercial vehicle entrances to enter FL. A physical search is required before allowing entrance to the installation.

(4) Non-affiliated personnel must demonstrate valid purpose for accessing installation. Sponsorship presence may be required for entrance to FL.

i. Contractors:

(1) Sponsoring organizations, activities, and persons will be responsible for monitoring contractor access by submitting a completed and approved DES Form 118 to the Installation All American VCC, detailing the contracted services to be performed, location of services, and duration of the contract.

(2) Contractors requesting access for less than one (1) year may receive an AIE visitor card on a case-by-case basis, or a temporary vehicle pass, not to exceed one (1) year. The expiration will be the end date of the contract or visit, or the expiration of the sponsor's access card, whichever occurs first.

(3) AIE card expirations may be updated to reflect a new contract period by submitting an approved DES Form 118 to the All American VCC. Renewed short term passes must be re-processed at the All American VCC.

j. Food Deliveries/Vendors (pizza deliveries, UPS, FEDEX, etc.):

(1) Vendors must apply for an AIE visitor pass at the All American VCC and will be run through NCIC III. Drivers must possess a valid state issued DL, state vehicle registration and proof of insurance.

(2) Vendor vehicles are subject to inspection prior to being granted access onto FL.

(3) Access control guards will randomly verify food deliveries by calling the customer (vendor must provide contact information). Deliveries must have an on-post destination.

(4) Media: Media personnel will always be escorted by a FL Public Affairs Office (PAO) representative.

(5) The PAO will notify the DASG Headquarters of their escort request. The DASG Headquarters is located at the DES building at the corner of Armistead and Butner Road.

(6) Media vehicles will be inspected before allowing entry to the installation. If required, the DL for each occupant will be run through NCIC III.

k. Directorate of Family, Morale, Welfare and Recreation (DFMWR) patrons. Non-DoD affiliated persons requesting access to participate in events, (i.e., hunting, fishing, bowling league, etc.), are required to complete a DES Form 118, or process at the All American VCC to receive a pass for one (1) year. AIE visitor cards will be issued not to exceed (1) year.

l. Pedestrians and Bicyclists. A 100% inspection of all bags and packages will be conducted of persons who do not possess a DoD ID card. Visitors must comply with procedures in para 16-2e.

m. Retired DoD Civilians and DA Civilian Family members, Army, and Air Force Exchange Service (AAFES) retirees and Family members will be granted access to FL under the following conditions:

(1) Civilian retirees must provide proof of retirement status (Civilian Retiree card).

(2) Civilian retirees/Family members without a valid DoD ID card must be sponsored and submit a DES Form 118 to the All American VCC, or process for an AIE visitor pass for one (1) year without sponsorship. Automated Installation Entry cards will be issued, not to exceed one (1) year.

n. School faculty, staff, and administrators must be sponsored and submit DES Form 118 to the All American VCC and possess/provide a school district ID card with valid state DL or state photo ID card when processing. AIE visitor cards will not exceed one (1) year.

o. Taxi Drivers (including UBER/LYFT, etc.). Must apply for an AIE visitor pass at the All American VCC for a period of one (1) year. Drivers must possess a valid DL, valid taxicab operator's "hack" license, vehicle registration, and proof of insurance.

(1) Vehicles are subject to be inspected before access to FL is granted.

(2) Inbound taxis drivers who are non-DoD affiliated will not be granted Trusted Traveler status even if their passenger is a DoD affiliated ID cardholder.

(3) Taxi drivers and passengers possessing a DoD affiliated ID card will be granted access as Trusted Travelers.

p. Non-Sponsored Tow Trucks. Tow truck drivers will be directed to the All American VCC for a pass.

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

(2) Vehicles being towed for maintenance reasons will be verified telephonically with the person(s) requesting the tow.

(3) Repossessions. Creditors, or their agents, requesting access to FL to recover property based on default of a contract or legal agreement are required to process at a VCC and receive a pass. Repossession agencies must coordinate through the PMO. The MP Desk will provide an escort and notify the Installation SJA. Re-possessors and/or affiliates are barred from entering the installation and other areas affiliated with FL at any time to facilitate repossessions without prior written authorization from the MP Station.

(4) The creditor or their agent must adhere to the following procedures:

(a) Copy of title, contract or legal agreement must be presented.

(b) Present evidence that the debtor is in default of the contract or legal agreement.

(c) Agents must present evidence they are working for the creditor.

(d) VCC personnel will notify the MP Desk Sergeant of any creditor/agent being processed for a pass.

(e) VCC personnel will inform creditor/agents to report to the MP Station and provide the documentation to the MP Desk Sergeant. The MP Desk Sergeant will have a MP patrol escort the creditor/agent to their location for their business. Creditor/agents are prohibited from attempting to repossess a vehicle without first reporting to the MP Desk. This includes any form of reconnaissance, scouting, investigation, and other means of exploration or searching for any property. This includes weather conducted by a paid or unpaid employee(s), use of company or personal means of conveyance, or other means.

q. Visitors/Guests of Residents. Non-DoD affiliated (without a DoD ID card) visitors or guests of a resident will:

(1) Apply for an AIE visitor pass, not to exceed one (1) year, without sponsorship at the All American VCC.

(2) Present their visitor ID (state DL or state ID w/photo) for verification through a background screening.

r. Family Care Providers are individuals who are a non-affiliated parent or guardian with custody of a Family member/child (dependent) who otherwise do not meet the requirements for issuance of a CAC or DoD card. The care provider will receive an ID as the sponsor and must:

(1) Receive a DA Form 1602 from the ID card issuing authority IAW AR 600-8-14.

(2) Process at the All American VCC and present their DA Form 1602 to the VCC registrar to receive an AIE card. This applies to caregivers who are sponsored as having an official purpose and are approved for access by the Installation Commander (IC) or his designated representative. Caregiver access cards will be issued, not to exceed one (1) year.

(3) If a DA Form 1602 is not issued, the sponsoring authority will submit a DES Form 118 to the Installation Access Control Officer certifying the person conducts caregiver services on FL. Caregiver visitor cards will be issued, not to exceed one (1) year.

s. Foreign National Visitors (Not On Military Orders):

(1) Foreign national visitors, traveling in the U.S., not on military orders are Not Authorized Unescorted Access to Fort Liberty. They are required to be sponsored by an adult authorized DoD ID cardholder utilizing a completed and approved DES Form 118 (Appendix N) and always escorted for access to FLNC.

(2) Forty-eight (48) hours in advance, the sponsor must submit a "Request for a Foreign National FL Installation Access Control Pass", DES FM 118, via an ".mil email," and must digitally signed and encrypt the email for the protection of the visitors' information (https://home.army.mil/liberty/application/files/4614/8131/2859/Installation_Badges_and_Passes_Request_DES_Form_118.pdf). The Form must be approved and signed by a Designated Representatives for Brigade/Group/Battalion/Squadron or higher CDRs, Executive Officers, Directors, Deputy Directors, or Contract Officer Representatives (CORs), as it applies to the sponsor and/or purpose of visit. The form can be hand delivered to the All American Visitor Center or email usarmy.liberty.id-readiness.list.id-readiness-list-des118@army.mil a completed and approved DES Form 118 to the FL DES/Physical Security Division,

Department of the Army Security Guards Army Security Guards (Chief of Guards), phone (910) 432-1200/1199. A VCC representative will contact and request the sponsored person(s) report to the VCC for issuance of their access card.

(3) Visitor passes may only be issued for up to 90 days. Copies of the ID documents for the visitor and DoD sponsor will be made at the Visitor Control Center. If the sponsor refuses to allow their identity documents to be copied a pass will not be issued and the foreign national visitor will be denied access to the installation.

(4) Foreign national visitors, excluding citizens of Canada and those visitors on military orders, are required to produce either a passport with a Form I-94, OR an I-551 (Permanent Resident Card, aka: "Green Card"). Foreign nationals from countries that are part of the Visa Waiver Program will be issued a Form I-94W or have a stamp placed in their passport. The I-94/I-94W or the stamp is issued to all foreign visitors by US Customs when they initially enter the US. These documents are required to be presented to receive a pass at the VCC. Note: Passports often include a VISA overprint in the internal pages. The status of the VISA is not a determining factor for installation access.

(5) The VCC will collect full data on foreign national visitors who are not on military orders. Copies of the passport and the accompanying I-94 or I-94W, or I-551 for Permanent Resident Aliens, military ID, orders, and any other pertinent documentation presented will be made and scanned into a portable document format (PDF) file.

(6) In addition to the information on the AIE visitor pass, the foreign national driver, and foreign national passengers of a vehicle, whether a sponsor is required or not, will have an AIE visitor pass/card completed IAW the AIE pass/card enrollment.

(7) Canadian citizens are only required to show some form of valid ID (e.g., DL and/or passport), an I-94 or I-551 is not required.

t. Foreign National Visitors (On Military Orders): Military personnel of foreign governments on orders for duty in the US, are only required to present their military ID card and their orders to the VCC registrar for passes, or they may submit an approved DES Form 118 for an AIE card, expiration will not exceed one (1) year.

u. Trusted Traveler Program (TTP):

(1) When authorized by the SC, the TTP allows active-duty service members and their spouses, military dependents 18 years or older, DoD employees, retired uniformed service members and their spouses to vouch for passengers in their immediate vehicle without showing an ID card, provided the Trusted Traveler vehicle operator possesses a valid DoD affiliated ID card.

(2) The TTP is not authorized for contractors, volunteers, or Family care providers.

(3) Trusted Travelers are entirely responsible for the actions of their passengers and for meeting all local security requirements for escort as established by AR and the SC.

(4) Vehicle passengers 18 years of age or older must be in possession of a valid photo ID card (i.e., DL, state ID, DD Form 1173, Uniform Services ID and Privilege card, DD Form 2 series, passport) so they may be readily identified while on FL.

(5) Passengers below the age of 18 who do not possess a valid photo ID card may be vouched for by an adult passenger of the vehicle who has been cleared to enter Fort Liberty.

(6) The TTP will be suspended at FPCONs Charlie and Delta or as directed by the SC.

v. Debarment. The SC may deny a person access for: involvement in the commission of a criminal offense; when access is inconsistent with the interests of National Security; when personal conduct reflects negatively on the image of the US; or when access adversely affects the health, safety, or morale of persons on Fort Liberty.

(1) Anyone debarred from FL may petition the SC (or delegated official) for partial or limited privileges.

(2) A CDR's recommendation to debar must be based upon investigative evidence, documented facts, and written coordination of the servicing SJA's office or legal representative when deciding if an incident is serious enough to warrant a debarment.

(3) Actions against Civilian employees will be coordinated through the servicing personnel office, and such action will be made a part of their official file.

(4) Actions to debar contractors from access to FL will be coordinated with the local contracting office.

(5) Under certain circumstances, limited debarments may be imposed on those who would otherwise receive installation debarment (i.e., person's still requiring access to their place of duty).

(6) Debarment information will be entered into the FL access control system.

(7) Physical Access Control System (PACS) will have the capability to display debarment status for registered persons.

(8) VCC access control guards will maintain a list of persons debarred from FL. All lists are For Official Use Only (FOUO).

(9) Local procedures will be used to update lists. Lists will not be released to the public and will be secured in areas that may not be viewed by unauthorized persons.

(10) Debarment lists may be combined and maintained in the same manner as lists used for tracking and documenting persons denied on-base driving or other privileges.

(11) ACP and VCC personnel will use the PACS or local debarment roster to ensure unauthorized persons are denied access, and if applicable, charged with trespassing when entry is illegally gained.

w. Persons with an Outstanding Warrant. The MP Desk will be notified of any person listed as having an outstanding warrant.

(1) Access will be denied unless the MP Desk has contacted the jurisdiction issuing the warrant and verified the warrant is no longer valid. (Note: The I2MC reporting that there is no warrant in NCIC is not sufficient).

(2) If the MP Desk is unable to verify the warrant has been cleared, the subject is to be informed of the following: "Our records show an outstanding warrant from (enter appropriate jurisdiction) (e.g., Cumberland County, Lee, Hoke, Robeson, etc.) and you will be denied access until the warrant has been cleared." VCC personnel will not relay the source of the information to the visitor (e.g., visitors will not be told the information comes from the Bars and Suspension List or from NCIC screening). Subjects are not authorized to view the information under any circumstances.

x. Persons with Conviction Records. The purpose of security screening is to ID those persons who may pose a threat to good order and discipline on FL by either denying them access or placing restrictions on their movement. The following criteria will be used as a guideline for determining denial of access to FL:

(1) Any record of a felony conviction regardless of the time period for a crime (includes murder, rape, sale of illegal drugs, grand theft, arson, and kidnapping).

(2) VCC personnel will not relay the source of the information to the visitor (e.g., visitors will not be told that the information comes from the Bars and Suspension List or from NCIC screening). Subjects are not authorized to view the information under any circumstances.

(3) The SC (or delegated official) is the final approval authority for any adjudication request for access denial.

y. In situations where a warrant is confirmed to be active and extradition is requested, installation security personnel (DA police, security guards, or military police) will detain the individual for the law enforcement agency. Persons with an active, confirmed warrant can be detained up to 3 hours pending the arrival and release to the extraditing agency. If the extraditing agency is unable to send an officer within 3 hours, arrangements with local law enforcement should enable custody transfer until the detainee can be released to the extraditing agency.

10-3. Special Event Access. The DoD requires all installations conduct a vetting process to determine fitness and eligibility for access. The two (2) categories of special events for DoD CAC holders and non- DoD ID cardholders are Installation and Hosted events.

a. Installation events are large functions (i.e., 4th of July, air shows, All American Week, concerts, etc.) where persons with no DoD credentials will be directed to specific gate(s) and security measures will be conducted prior to entrance onto the installation.

(1) The SC or GC will determine which events are Installation Events.

(2) A NCIC III screening for non-DoD personnel attending an installation event will be waived where screening is impractical.

(3) All non-DoD personnel 18 years and above are required to present a valid state photo ID.

(4) All motor vehicle operators are required to present a valid DL, registration, and proof of insurance.

(5) Vehicles are subject to a 100% search before being allowed access to the installation.

b. Hosted events are small functions on the installation where DoD sponsors have the option to submit a special event access request for persons who will be in attendance and who do not possess DoD credentials (e.g., weddings, proms, promotion ceremonies, retirements, Family reunions, birthdays, personal gatherings, etc.). Such persons will be directed to specific gate(s) where security measures will be conducted prior to entrance onto the installation.

(1) To host a non-military group from off base, the DoD sponsor must contact the VCC or email usarmy.Liberty.imcom-atlantic.mbx.allamerican-vcc@mail.mil to request approval. The request must be made 14 days in advance, but no later than 10 duty days prior to the event.

(2) The request must contain the following information: Description of event, time/duration of event, location of event, and approximate number of non-DoD attendees.

(3) A minimum of 25 visitors are required to make a hosted special event request or otherwise the non-DoD visitors will need to obtain a visitor pass at the All American VCC.

(4) Forty-eight (48) hours in advance, the sponsor must submit a "Request for a FL Installation Access Control Badge", DES FM 118, via an ".mil email," and must digitally sign and encrypt the email for the protection of the visitors' information. The guest event access list must contain the following information for each guest over 18 years of age not possessing a valid DoD access credential:

(a) Official Name: (Last, First, M.I.).

(b) Grade/Rank/Status (e.g., Civilian (CIV), Staff Sergeant (SSG)).

- (c) Gender (Male/Female).
- (d) Sponsor's Organization/Agency.
- (e) Organization Phone Number.
- (f) Relationship to Sponsor.
- (5) Ensure guests have a valid form of ID (e.g., DL or state ID) to present at the ACP.

(6) The approved event list will be provided to the selected ACP for a specified period of time for verification of guests on the day of the event. Guests arriving outside the specified period of time will proceed to All American VCC for normal access pass.

(7) A 100% vehicle search will be conducted at designated ACPs.

(8) Upon the completion of the event all special event guests are required to depart the installation in a timely manner.

(9) All guests have the option to obtain an unescorted visitor's pass for one (1) year. This can be accomplished by going to the All American VCC and processing in person in advance of the event date. The pass can be used for access to the installation at any ACP.

Chapter 11

Personnel Reliability Program

11-1. 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. The following positions or duties in Army physical policies require a determination of reliability:

- a. Unaccompanied access to arms, ammunition, and explosives per AR 190-11.
- b. Unaccompanied access to controlled medical substances per AR 190-51.
- c. Employment and retention as a DA police officer or DA security guard, per AR 190-56.

11-2. 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.

11-3. Contractors. 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.

11-4. Instructions and use of the DA Form 7708. The DA Form 7708 (Personnel Reliability Screening and Evaluation Form) with instructions on use in 190-13 (para 2-21), is/will be used to document the reliability determination process. For submission of a Police Records Check email the document to Police Services at usarmy.Liberty.imcom-atlantic.mbx.police-services@mail.mil.

11-5. 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.

11-6. Continuous evaluation. It is essential to continually evaluate personnel in this program. Any incident/problem that might be cause for temporary/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/allegation about a person's suitability under this program. Verbal or telephonic notifications will be confirmed in writing.

11-7. 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.

11-8. 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 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.

11-9. Personnel interview. The certifying official will interview the person to appraise character, judgment, reliability, attitude, emotional and mental maturity, and sense of responsibility. Those exhibiting financial irresponsibility will not be selected. Interviews will be documented on DA Form 7708, which will be completed per this regulation.

11-10. Annual review. The reliability determination will be reviewed every year in the on-boarding month or a change of status (for example, departs the unit, criminal activity whether alleged or adjudicated).

Chapter 12

Security of Aircraft and components. Army aircraft and components Army aviation facilities and not at Army aviation facilities will both be secured per AR 190-51, all applicable security physical protective measures, security procedural measures (risk levels), and physical protective measures.

a. Army aircraft with arms, ammunition, and explosives (AA&E) aboard will be secured per AR 190-51, AR 190-11, and this regulation.

b. When not in use, aircraft containing weapons will be parked inside an aircraft parking area. The parking area will be lighted and will have either continuous surveillance or an IDS on the perimeters to detect aggressor before they access the aircraft.

c. When operational readiness permits, weapons mounted on aircraft that are accessible and easily removable will be removed and stored in a secure location. Weapons that remain installed on the aircraft will be made inoperable by removing barrels or firing mechanisms when practical in accordance with AR 190-11.

d. Removed components will be stored in a secured location. A secured location is an arms room, an ammunition supply point, an area under continuous armed surveillance, or any structure meeting the requirements for storage of category I or II AA&E in AR 190-11.

e. Additional security for accessible and easily removable components will be by storage in a secure structure per 190-51.

f. U.S. Army aircraft with classified materials aboard will be secured per AR 380-5. Classified materials which can be readily removed will be placed in secure storage per AR 380-5.

g. The requirements in this paragraph apply to unmanned aircraft systems over 20 pounds (for example, RQ-4 Global Hawk, MQ-1 Predator, and Sky Warrior) and maintained in aircraft parking areas/hangars.

Unmanned aircraft systems under 20 pounds (for example, RQ-11 Raven, RQ-14 Dragon Eye) will be secured per R 190-51.

Appendix A References

Section I Required Publications

DoDM 5100.76

Physical Security of Sensitive Conventional AA&E

DoDD 3020.40

Mission Assurance

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 95-1 Flight Regulations

Appendix A - Continued

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 525-26

Infrastructure Management

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

Appendix A - Continued

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 Liberty Reg 385-64

Explosive Safety Management Program

Fort Liberty 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

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

Appendix A – Continued

DA Form 5513

Key Control Register and Inventory

DA Form 5557

Individual Reliability Screening and Evaluation Record

DA Form 7278-R

Risk Level Worksheet

SF Form 700

Security Container Information

SF Form 701

Activity Security Checklist

SF Form 702

Security Container Check Sheet

Fort Liberty Form 975-E

Intrusion Detection System (IDS) Personal Identification Code (PIC) Request Form

Fort Liberty Form 2488-E

Weapons, Ammunition, Sensitive Items and Key Count/Inventory

Fort Liberty Form 2488-3E

Monthly Serial Number Inventory of Weapons and Ammunition

Fort Liberty Form 2488-3A-E

Monthly Serial Number Inventory of Weapons and Ammunition (Continuation)

Fort Liberty Form 2488-4E

Ammunition Surveillance Inspection Record

**Appendix B
Alarm System Test Record**

ALARM SYSTEM TEST RECORD					
UNIT/ACTIVITY			INSTRUCTIONS: Contact the I2MC at (910) 396-3071; announce your intentions to conduct your monthly alarm test. Provide the monitor with building zone # and validate who you are prior to proceeding with test. Remain on the line until directed otherwise by the I2MC.		
BUILDING/ROOM/ZONE #					
CUSTODIAN					
DATE	TIME	INITIATED BY	RECEIVED BY	TEST RESULT	CORRECTIVE ACTION

Appendix C
Sample Appointment Order for Unit Crime Prevention Officer

Unit Letterhead

Office Symbol
MEMORANDUM FOR SEE DISTRIBUTION

Date

SUBJECT: Crime Prevention Officer Primary and Alternate

1. The following individuals are hereby appointed as Crime Prevention Officers for (BDE/SQDN/BN/Co/Trp/Btry).

<u>Name</u>	<u>Rank</u>	<u>Position</u>
Jones, I. C.	SSG	Primary
Tardy, I. Am.	SGT	Alternate

2. Effective Date:

3. Authority: AR 190-13

4. Period: Until officially relieved or released from appointment or assignment.

5. Special Instructions: Perform the assigned duties IAW the BDE/SQDN/BN/Co/Trp/Btry/Sqdn) Crime Prevention SOP.

6. POC for this memorandum (list name and telephone of POC).

BDE/SQDN/BN/Co CDR Signature Block

Appendix D
Sample Unit Crime Prevention Program SOP

Unit Letterhead

Office Symbol

Date

SUBJECT: Unit Crime Prevention Standing Operating Procedures (SOP)

1. Purpose. To establish and prescribe policies and procedures for assigning responsibilities and provide guidance concerning security of personal and military property and reduce criminal activity risks involving personnel and property within the higher headquarters and subordinate commands.
2. References:
 - a. AR 190-13, The Army Physical Security Program, 27 Jun 19
 - b. AR 190-51, Security of Unclassified Army Property (Sensitive & Non-Sensitive), 27 Jun 19
 - c. AR 710-2, Supply Police below the National Level, 28 March 08
 - d. DA Pam 190-51, Risk Analysis for Army Property, 30 September 93
 - e. DA Pam 710-2-1, Using Unit Supply System (Manual Procedures), 1 December 16
 - f. Fort Liberty Regulation 190-13-1, Fort Liberty Physical Security Program, 2020
3. Applicability. This policy applies to all unit personnel, 1 June 2015
4. Responsibilities:
 - a. Commander:
 - b. CPO Primary/Alternate:
 - c. Soldier:
 - d. Unit Supply:
 - e. Staff Duty Officer/Noncommissioned Officer:
 - f. Charge of Quarters:
5. Personal Property
6. Unit Storage
7. Inventory of Personal Property/High Value Items
8. Marking of Personal and Government Property
9. Electric Engravers and other Tools

Appendix D - Continued

10. Prohibited Weapons
11. Illegal Drugs
12. Health and Welfare Inspections
13. Visitor Policy
14. Rape Prevention/Treatment of Rape Victims
15. Reporting a Crime or Suspicious Activity
16. Security Measures for Privately Owned Vehicles
17. Off Limit Areas
18. North Carolina Drinking Law/Drinking While Intoxicated (DWI)
19. Light Control Measures

CDR's Signature Block

**Appendix E
Crime Prevention Briefing Checklist**

Unit Letterhead

Office Symbol

Date

SUBJECT: (LIST UNIT) CRIME PREVENTION BRIEFING CHECKLIST

I, _____ received a unit Crime Prevention
(Print Last Name, First Name, MI)
briefing/orientation which included the following topics:

<u>TOPICS</u>	<u>YES</u>	<u>NO</u>
Unit Crime Prevention Policies	_____	_____
Procedures for Securing Personal Property	_____	_____
Personal Property Record/Inventory of High Value Items	_____	_____
Accessibility and Location of Electric Engravers (or other tools)	_____	_____
Visitor's Policy	_____	_____
Local Trouble Spots	_____	_____
Prohibited Weapons/Items and Drug Paraphernalia	_____	_____
Off Limit Areas	_____	_____
Procedures to Report a Crime or Suspicious Activity	_____	_____
North Carolina State Drinking Law/Drinking While Intoxicated (DWI)	_____	_____

(Signature of Soldier)

(Date)

Appendix F
Arms Room Closeout/Pre-Occupancy Procedures

ARMS ROOM CLOSE OUT PROCEDURES

1. The following procedures are required by Commanders (CDRs)/Facility Managers (FM) when closing out an arms room due to a deployment:
 - a. Place ICIDS alarm in "ACCESS" mode once the arms room has been 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.
 - b. 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.
 - c. 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 at the DES Bldg. 2-5935, Room 115 (intersection of Butner Road and Armistead Street).
2. Pre-occupancy for re-deploying units is required before the occupation of an arms room.

ARMS ROOM PRE-OCCUPANCY PROCEDURES

1. Contact the ICIDS Administrator at (910) 396-1946 to ensure the activation of the ICIDS system prior to scheduling a pre-occupancy inspection.
2. Contact the IPSO at (910) 396-9109 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 Fort Liberty Form 975-E (must include current/new armorers, and new building number and zone ID#). Failure to submit current armorers on the new FL Form 975 will result in them not having access to the new zone. Current armorers will transfer their PICs to the new zone. Note: Fort Liberty Form 975-E must be completed on-line and digitally signed.
 - c. DA Form 7708, Personnel Reliability Screening and Evaluation (required for new armorers). A copy of existing DA Forms 7708 on file for current armorers is not required.
 - d. Current copy of CDR's assumption of command memorandum.

Appendix G
Controlled Substance Record

CONTROLLED SUBSTANCES RECORD For use of this form, see AR 40-3; the proponent agency is OTSG.		This form is to be used in conjunction with DA Form 3949-1		WARD/CLINIC		DATE INITIATED (YYYYMMDD)				
MONTH/YEAR	ITEM (Generic Nomenclature; may add trade name for additional clarity)	ACCOUNTABLE UNIT	FORM INITIATED (Sign and Print Name)			BALANCE FORWARDED (From the previous sheet)				
DAY	HOUR	PATIENT NAME (Last Name, First Name)	ORDERED BY (Dr.'s Last Name)	ADMINISTERED BY (Sign on top line; Print name on bottom line)	WITNESS TO ANY WASTE (Sign on top line; Print name on bottom line)	ACTUAL DOSE ADMINISTERED TO PATIENT	AMOUNT OF MEDICATION WASTED	EXPENDITURES (Accountable units used)	RECEIPTS (Amount from pharmacy)	BALANCE (Accountable Units Remaining)

DA FORM 3949, SEP 2009 PREVIOUS EDITIONS ARE OBSOLETE. APD PE v1.00

Appendix I
Intrusion Detection System (IDS) Personal Identification Code (PIC) Request Form

INTRUSION DETECTION SYSTEM (IDS) PERSONAL IDENTIFICATION CODE (PIC) REQUEST FORM					
For use of this form see FL Reg 190-13-1; the proponent is DES, Physical Security					
PRIVACY ACT STATEMENT					
AUTHORITY:		Title 5, U.S.C. Section 301			
PRINCIPAL PURPOSE:		To provide information on individuals authorized access to ICIDS protected facilities.			
ROUTINE USES:		Validate security requirement.			
DISCLOSURE:		Voluntary, however authority to process access will be withheld from individuals who do not provide information.			
SECTION A - UNIT INFORMATION (Must be fully completed)					
1. Unit/Activity Address: (Complete physical address)		2. To: ICIDS Administrator Physical Security Division Fort Liberty, NC 28310		3. Date: (dd/mmm/yyyy)	
4. Bldg #:	5. Zone ID # A	6. Asset Cat. AA&E	7. Street/Road:	8. Cross Reference Street(s):	
SECTION B - ON-CALL/AFTER HOURS ORGANIZATIONAL CONTACTS (Information is required)					
1. Staff Duty Phone:		2. Brigade/Group Staff Duty Phone:			
SECTION C - PIC AUTHORIZATION (Must include all personnel authorized to receive PICs e.g., primary and alternate(s) custodian(s))					
Last Name	First Name	MI	Grade	Last 4 of SSN	Contact Phone #
SECTION D - Commander's/Facility Manager's Certification (Must be signed by Commander/Facility Manager only)					
1. Signature:		2. Date: (dd/mmm/yyyy)		3. Phone:	

FL 975 IDS PIC FORM JUN 2023 (AMIM-LIL-ESS) PREVIOUS EDITIONS ARE OBSOLETE

INSTRUCTIONS FOR COMPLETING IDS PIC REQUEST FORM

1. Purpose. This form is used to identify ICIDS locations, list emergency after duty hour POCs, and to issue PICs for ICIDS protected facilities. This form is to be generated anytime there is a change of personnel, to include but not limited to; change of commander (CDR) facility manager (FM), PIC holder resulting from PCS, ETS or at anytime there is an actual or suspected sharing or compromise of a user's PIC.

2. Prohibited Use of PICs. The actual or suspected sharing of PICs is **strictly prohibited** and will result in the immediate deletion of the user's PIC in question and may result in non-judicial punishment or disciplinary action.

3. General Instructions:

- a. Previous versions of this form are obsolete and will no longer be accepted.
- b. An updated DES IDS PIC Form will result in the immediate deletion of all PICs for the ICIDS facility previously listed on the superseded form.
- c. All information on the DES IDS PIC Form must be legible and completely filled out.
- d. ICIDS protected facilities must have a primary and at a minimum one alternate custodian.
- e. Host CDRs of consolidated arms rooms must sign a consolidated DES IDS PIC form for each separate unit's personnel requiring a PIC.
- f. The original DES IDS PIC Form will be submitted to the ICIDS Administrator for processing. A copy will be retained by the organization in the ICIDS protected area IAW regulatory requirements. Personnel listed on DES IDS PIC form must be listed on the organization's Unaccompanied Access List/Roster.
- g. PIC issuance requires the following documents:
 - (1) Completed DES IDS PIC Form (must be completed and legible).
 - (2) Completed DA Form 7281-R, Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Records (Background check).
 - (3) Valid military or DoD identification card.
 - (4) Copy of the Commander's/Facility Manager's Assumption of Command Orders, if there has been a change of Commander/Facility Manager.

4. Specific Instructions:

- a. **Section A - (Unit Information):**
 - (1) Unit/Activity Address: Type the unit/activity responsible for the facility. Example: A Co, 123rd Bn, etc.
 - (2) DES Address
 - (3) Date: Enter as dd/mmm/yyyy.
 - (4) Bldg #: Enter the building number in which the facility is located.
 - (5) Zone ID #: This is normally the building designator associated with the ICIDS facility, ie., A, B, C, D, etc.
 - (6) Asset Category: Select from drop down box applicable asset, ie., AA&E, COMSEC, Fund Storage, etc.
 - (7) Street/Road: Enter the nearest street name to the protected facility.
 - (8) Cross Reference Street(s): Enter the nearest intersecting or cross street (may be located two or three blocks away).
- b. **Section B - (On-Call/After Hours Organizational Contacts):**
 - (1) Staff Duty Phone: Enter the phone number for the Staff Duty/NCO and, if available, a pager number.
 - (2) Brigade/Group Staff Duty Phone.
- c. **Section C- (PIC Authorization)**

Enter the Last, First Name, Middle Initial, Grade, last 4 of SSN and a contact telephone number of person(s) requiring a PIC.
- d. **Section D- (Commander's/Facility Manager's Certification):** Self explanatory.

Appendix J
Special Event Access Attendee List

SPECIAL EVENT ACCESS ATTENDEE LIST
EVENT NAME: _____

Name (Last, First, M.I.)	Grade/Rank/ Status	Gender (Male/Female)	Sponsoring Organization/Agency	Organization Phone #	Relationship to Sponsor (Spouse/Dependent/ Friend, etc.)

Appendix K

Physical Security Inspection Program

1. The Physical Security Inspection program is a systematic approach to the execution of the Physical Security Evaluation objectives on a recurring 18-month calendar.
2. Exceptions and waivers to the Inspection program must be approved by the IPSO.
3. A physical security inspection is a formal recorded assessment of the physical protective measures and security procedural measures implemented to protect government assets. There are two (2) required inspection periods for critical asset categories at 18 and 24 months IAW AR 190-13, The Army Physical Security Program, dated 27 June 2019. The program combines these intervals into an 18-month requirement for unit predictability during long range planning.
4. Installation Physical Security Officers.
 - a. At a minimum, inspections will comply with assets listed in the 190-series of Army regulations.
 - b. Ensure physical security inspections are recorded and analyzed using the Army Security Management System (SMS).
 - c. Ensure a copy of the physical security inspection report is provided to the CDR/DIR/FM, and the higher CoC of the unit inspected within five (5) working days.
 - d. Track recurring deficiencies during future physical inspections until corrected.
 - e. If the initial inspection resulted in an unsatisfactory rating, ensure follow-up inspections are conducted six (6) months later, IAW AR 190-13 and AR 190-11.
5. Directorate of Plans, Training, Mobilization, and Security (DPTMS) will distribute the approved 18-month inspection plan to Garrison, and coordinate with XVIII Airborne Corps G3 to distribute to all Fort Liberty mission units and tenant organizations.
6. Commanders/Directors/Facility Managers.
 - a. Provide the unit/organization PSO contact information to the Physical Security Office at (910) 396-9109, a minimum of 30 days prior to the scheduled inspection date.
 - b. Contact the IPSO for scheduling conflicts. Requests for exceptions must be submitted to the IPSO and must be approved through the first COL/O6 or equivalent in the unit's/organization's chain of command.
 - c. Provide a report of action taken for inspections with unsatisfactory ratings to the Installation Physical Security Office within 30 workings days from the date of the inspection.
7. Procedures.
 - a. Physical security inspections will be conducted on weekdays, between the hours of 0900 to 1600.
 - b. At a minimum, the following personnel must be readily available during the inspection process:
 - (1) Unit CDR or designee (must be able to sign for CDR).
 - (2) Facility manager (if applicable)

Appendix K - Continued

- (3) Physical Security Officer/Unit S2
- (4) Arms Room Officer
- (5) Armorers (for consolidated arms rooms, all armorers are required to be present)
- (6) Supply Officers
- (7) Motor Pool Officer or NCOIC
- (8) Communications Officer or NCOIC
- (9) Pharmacy Supervisor (if applicable)
- (10) Airfield Manager (if applicable)
- (11) School Principal (if applicable)

8. Ammunition licenses, pre-occupancy/post occupancy inspections will be conducted on Fridays. In the event a training day or holiday falls on a Friday, inspections will be conducted on Thursdays.

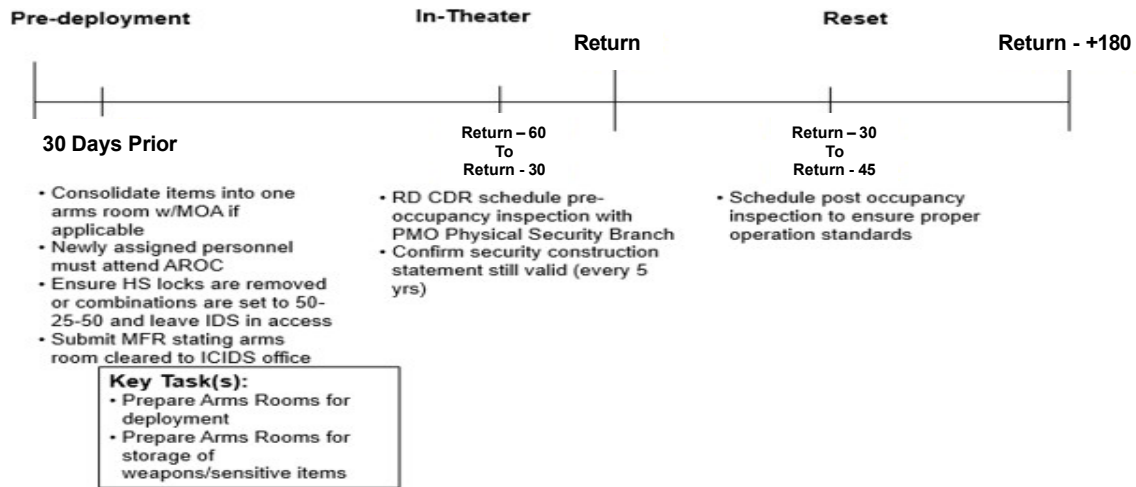
9. A copy of the Physical Security 18-month Long Range calendar may be obtained through the XVIII Airborne Corps G3 or through the IPSO at (910) 396-9101.

Appendix L ICIDS Alarm System Test Procedures

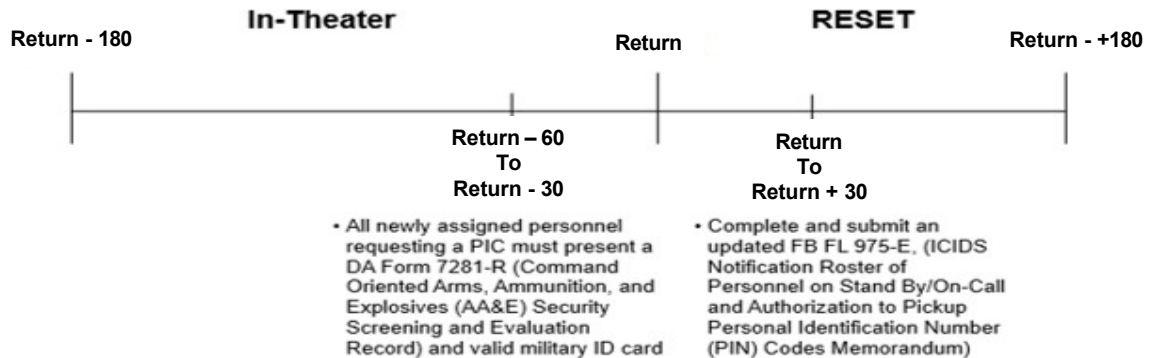
1. Monthly Walk/Duress Check. The monthly walk and duress checks will be conducted by all alarm zones and logged by the armorer or custodian, and the alarm monitor (AM).
2. Alarm systems will be tested monthly by an authorized personal identification code (PIC) holder of each facility. The custodian conducting the test must authenticate with the AM prior to entry or executing the test. 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. A common mistake during these tests is the custodian arming, testing and then disarming the system before completion of the delay timer. 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. 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. 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 90 days.
4. I2MC/alternate I2MC. The I2MC/alternate I2MC will be tested quarterly, depending on which post is manned. The alternate alarm-monitoring site will be tested once a month. While the alternate I2MC is operational, utilize the PMO armory to conduct a 100% check of all alarm points.
5. Refer to AR 190-13, app H for ICIDS detailed operational test instructions.

**Appendix M
AA&E Pre-Deployment/Redeployment/Reintegration Procedures**

AA&E Pre-Deployment/Redeployment/Reintegration Procedures



Integrated Commercial Intrusion Detection System Codes



Key Task(s):

- Prepare Arms Rooms for storage of weapons/sensitive items

POC: Physical Security Division
396-9109

**Appendix N
DES Form 118 (Request For A Fort Liberty Installation Access Control Pass)**

REQUEST FOR A FORT LIBERTY INSTALLATION ACCESS CONTROL PASS

PRIVACY ACT ADVISEMENT: The information requested is for the purpose of granting access to the Fort Liberty Installation. Providing requested information, to include your social security number (SSN), is voluntary. However, your access may not be granted if all requested information is not provided. **AUTHORITIES:** Executive Orders (EO) 10450, 10865, and 12333. The SSN, required for record accuracy, is requested pursuant to EO 9397.

1. APPLICANT INFORMATION:

LAST Name: _____ FIRST Name: _____ MIDDLE Initial: _____
 Grade/Rank/Status: _____ SSN#/Passport#: _____ DOB: _____
 Gender Male Female Driver's License # _____ Country of Origin: _____
 Organization/Unit: _____ Phone Number and Cell #: _____
 E-Mail Address: _____ Relationship to Sponsor: _____

2. REQUESTED BADGE: Non-DoD Contractor Foreign National Friend Partners of Liberty
 Vendor Family Care Provider/Au Pair

Requested Date(s)/Time(s) of Visit: _____
 Contract Period (from/to dates) Contractor/Vendor use as applicable: _____

3. JUSTIFICATION FOR BADGE/PASS:

4. SPONSOR INFORMATION: LAST Name: _____ FIRST Name: _____
 MIDDLE Initial: _____ Grade/Rank/Status: _____ DOB: _____
 Gender: Male Female Driver's License # _____ DOD ID # _____
 Organization/Unit: _____ Organization/Unit Phone Number: _____
 E-Mail Address: _____

5. COMMANDER'S/DIRECTOR'S/FACILITY MANAGER'S CERTIFICATION:

I certify that the applicant meets the justification requirements as indicated in paragraph 3 above for access privileges. Furthermore, I certify that the applicant requires an access control badge/or pass indicated above in order to perform assigned duties or conduct official business on Fort Liberty.

 BDE/BN CDRs, XO/Directors, Deputy Directors/
 Contracting Officer Representative
 (Invalid if incomplete)

 Printed Name/Rank/Telephone No.
 (Invalid if incomplete)

 E-Mail Address:
 (Invalid if incomplete)

SECTION BELOW IS FOR USE BY THE INSTALLATION ACCESS CONTROL OFFICE ONLY

6. ISSUING OFFICIAL:

Approved/Disapproved (circle one) _____

 Issuing Official Printed Name Issuing Official Signature
 Date: _____

Appendix O Restricted Areas

1. General.

a. This app 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 are per AR 190-13, 190-51, and this regulation.

d. Commercial imaging surveillance by photography or 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 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 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

Appendix O - Continued

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 per figure 2–1 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.

Appendix O - Continued

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 (910) 396-0392 and the Chief of Installation Physical Security will be notified.

e. Facts concerning a deliberate violation of a restricted area will be immediately reported per AR 381–12.

f. Photographing and sketching defense installations. Covered under and located at 18 U.S.C. § 795 - U.S. Code - Unannotated Title 18. Crimes and Criminal Procedure § 795., Photographing and sketching defense installations and reads:

(1) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

Appendix O - Continued

(2) Whoever violates this section shall be fined under this title or imprisoned not more than one (1) year, or both.

**Appendix Q
 Monthly Serial Number Inventory of Weapons and Ammunition (cont'd), (FL Form 2488-3A-E)**

Page of Pages

MONTHLY SERIAL NUMBER INVENTORY OF WEAPONS AND AMMUNITION (Cont'd)									
Type Weapon	Serial Number	Present	Not Present	Remarks	Type Weapon	Serial Number	Present	Not Present	Remarks

FL FORM 2488-3A-E, 12 JUL 23 (IMSE-LIL-ESM)

**Appendix R
Weapons and Ammunition, Sensitive Items, and Key Count/Inventory (FL Form 2488-E)**

WEAPONS, AMMUNITION, SENSITIVE ITEMS, AND KEY COUNT/INVENTORY															
For use of this form, see AR 190-11; the proponent agency is PMO.															
1. Type of Weapon													5. Key	Signature of Persons Relieved & Accepting Custody of Arms Room & Arms Room Keys	DATE:
2. In Arms Room														6. Relieved:	TIME:
3. Signed Out															DATE:
4. Total														7. Accepted:	TIME:
2. In Arms Room														6. Relieved:	DATE:
3. Signed Out														7. Accepted:	TIME:
4. Total															DATE:
2. In Arms Room														6. Relieved:	TIME:
3. Signed Out														7. Accepted:	DATE:
4. Total															TIME:
2. In Arms Room														6. Relieved:	DATE:
3. Signed Out														7. Accepted:	TIME:
4. Total															DATE:
2. In Arms Room														6. Relieved:	TIME:
3. Signed Out														7. Accepted:	DATE:
4. Total															TIME:
REMARKS															

Appendix S
Fort Liberty Local Records Check request



DEPARTMENT OF THE ARMY
XVIII AIRBORNE CORPS PROVOST MARSHAL OFFICE
BLDG 2-5634 STINER ROAD
FORT LIBERTY, NC 28310-5000

AMIM-LIL-PS

MEMORANDUM FOR: All persons requesting a Fort Liberty Military Criminal History Check on themselves or the below person.

SUBJECT: Fort Liberty Local Records Check

1. Name: _____

2. SSN: _____

3. Results:

No Record: Record:

Subject of a Report (Report# / Offense / Date):

4. POC is the undersigned.

(Provost Marshal Stamp/Date)

Appendix T
Use and instructions on completing DA Form 7708

1. **General.** Refer to AR 190-13 (app H) for use and instructions on completing DA Form 7708.

FOUO

PERSONNEL RELIABILITY SCREENING AND EVALUATION			
<small>For use of this form, see AR 190-13; the proponent agency is OPMG.</small>			
PRIVACY ACT STATEMENT			
Authority:	10 USC 3013 Secretary of the Army; DOD 5200.08, Security of DODI Installations and Resources and the DOD Physical Security Review Board; AR 190-13, The Army Physical Security Program; and E.O. 9397 (SSN) as amended.		
Principal Purpose:	To evaluate the qualification and suitability of a person for assignment to sensitive duties or unaccompanied access to certain resources.		
Routine Uses:	In addition to those disclosures generally permitted under 5 U.S.C. 552 a(B) of the Privacy Act, this information can be shared with local law enforcement agencies for criminal background checks.		
Note:	This system of records may contain personally identifiable health information (PHI). The DoD Health Information Privacy Regulation (DoD 5025.18-R) issued pursuant to the Health Insurance Portability Act of 1996, applies to most such health information. DoD 5025.18-R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974, as amended, or mentioned in this system of records notice.		
Disclosure:	Voluntary, however failure to provide all or part of the requested information may result in a non-selection for the stated duties.		
Citation:	AD690-200 DAPE Department of the Army Civilian Personnel Systems (January 06 2004, 69 FR 790); and A0600-8-104 AHRC, Army Personnel System (APS) (July 30 2013, 78 FR 45914).		
PART I - IMMEDIATE SUPERVISOR/COMMANDER INTERVIEW			
1. NAME (Last, First, MI)	2. ORGANIZATION	3. POSITION TITLE	4. SSN
5. I <input type="checkbox"/> DO <input type="checkbox"/> DO NOT OBJECT TO PERSONNEL SCREEN REQUIREMENTS.			
6. SCREEN FOR			
<input type="checkbox"/> Unaccompanied access to arms, ammunition and explosives		<input type="checkbox"/> Unaccompanied access to control medical substances	
<input type="checkbox"/> Employment/Retention as DA Civilian Police or Security Guard		<input type="checkbox"/> Issuance of Physical Security Inspector Credentials	
<input type="checkbox"/> Other (specify) _____			
7. SIGNATURE		8. DATE (YYYYMMDD)	
9. INTERVIEWER (Last, First, MI)		10. SIGNATURE	11. DATE (YYYYMMDD)
PART II - CHECK OF PERSONNEL RECORDS			
12. POTENTIALLY DISQUALIFYING INFORMATION WAS		<input type="checkbox"/> FOUND AND FORWARDED TO THE CERTIFYING OFFICIAL <input type="checkbox"/> NOT FOUND	
13. NAME (Last, First, MI)	14. SIGNATURE	15. DATE (YYYYMMDD)	
PART III - CHECK OF SECURITY RECORDS			
16. POTENTIALLY DISQUALIFYING INFORMATION WAS		<input type="checkbox"/> FOUND AND FORWARDED TO THE CERTIFYING OFFICIAL <input type="checkbox"/> NOT FOUND	
17. PERSONNEL SECURITY INVESTIGATION (PSI): COMPLETED ON DATE (YYYYMMDD) _____			
TYPE (NACLC, ANACI, SSBI, etc.) _____		<input type="checkbox"/> FAVORABLY ADJUDICATED <input type="checkbox"/> DOSSIER REVIEW REQUIRED	
18. PSI REQUEST OR REINVESTIGATION (IF REQUIRED): SUBMITTED ON DATE (YYYYMMDD) _____			
TYPE (NACLC, ANACI, SSBI, etc.) _____			
19. SECURITY CLEARANCE: <input type="checkbox"/> NONE <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> SECRET <input type="checkbox"/> TOP SECRET <input type="checkbox"/> NOT REQUIRED			
20. NAME (Last, First, MI)	21. SIGNATURE	22. DATE (YYYYMMDD)	
PART IV - CHECK OF MEDICAL RECORDS			
23. POTENTIALLY DISQUALIFYING INFORMATION WAS		<input type="checkbox"/> FOUND AND FORWARDED TO THE CERTIFYING OFFICIAL <input type="checkbox"/> NOT FOUND	
24. NAME (Last, First, MI)	25. SIGNATURE	26. DATE (YYYYMMDD)	
PART V - CHECK OF LAW ENFORCEMENT RECORDS			
27. POTENTIALLY DISQUALIFYING INFORMATION WAS		<input type="checkbox"/> FOUND AND FORWARDED TO THE CERTIFYING OFFICIAL <input type="checkbox"/> NOT FOUND	
28. NAME (Last, First, MI)	29. SIGNATURE	30. DATE (YYYYMMDD)	
PART VI - RESULTS OF RANDOM/DIRECTED DRUG TESTING			
31. TESTS RESULTS WERE:			
<input type="checkbox"/> FORWARDED TO THE CERTIFYING OFFICIAL		<input type="checkbox"/> CERTIFIED NEGATIVE <input type="checkbox"/> NOT A TESTING-DESIGNATED POSITION	
32. NAME (Last, First, MI)	33. SIGNATURE	34. DATE (YYYYMMDD)	

DA FORM 7708, JUN 2019

Page 1 of 2
 APO AEM v1.00ES

Appendix T - Continued

FOUO

PART VII - IMMEDIATE SUPERVISOR/COMMANDER EVALUATION/ BRIEFING		
35. AFTER A THOROUGH REVIEW OF INFORMATION PROVIDED, I FIND THE PERSON: <input type="checkbox"/> SUITABLE FOR THE POSITION/DUTY <input type="checkbox"/> UNSUITABLE FOR THE POSITION/DUTY		
36. I HAVE BEEN BRIEFED ON MY DUTIES AND UNDERSTAND THE STANDARDS.	37. SIGNATURE <small>(SEE NAME)</small>	38. DATE (YYYYMMDD)
39. NAME OF CERTIFYING OFFICIAL (Last, First, MI)	40. SIGNATURE <small>(SEE NAME)</small>	41. DATE (YYYYMMDD)
PART VIII - CONTINUING PERIODIC EVALUATION		
Document changes in the individual's status and/or administrative data. Attach a continuation sheet if additional room is required to document an update. Follow guidance in the pertinent regulation for documentation requirements for restriction, suspension, administrative termination, or disqualification. (ATTACH BLANK SHEET FOR CONTINUATION OF PART VIII)		
42. PERSON'S SIGNATURE/ DATE	43. CERTIFYING OFFICIAL'S SIGNATURE/DATE	44. REASON FOR UPDATE
<small>(SEE NAME)</small>	<small>(SEE NAME)</small>	
<small>(SEE NAME)</small>	<small>(SEE NAME)</small>	
<small>(SEE NAME)</small>	<small>(SEE NAME)</small>	
<small>(SEE NAME)</small>	<small>(SEE NAME)</small>	
<small>(SEE NAME)</small>	<small>(SEE NAME)</small>	
PART IX - SUSPENSION OR TEMPORARY DISQUALIFICATION (PENCIL ENTRY)		PART X - ADMINISTRATIVE TERMINATION
45. EFFECTIVE DATE (YYYYMMDD)		46. EFFECTIVE DATE (YYYYMMDD)
PART XI - DISQUALIFICATION		
47. STATUS AT TIME OF DISQUALIFICATION <input type="checkbox"/> 1. Being screened for _____ <input type="checkbox"/> 2. Assigned to/as: <input type="checkbox"/> a. Unaccompanied access to AA&E <input type="checkbox"/> b. Unaccompanied access to controlled medical substances <input type="checkbox"/> c. DA Civilian Police or Security Guard <input type="checkbox"/> d. Other _____		48. REASON FOR DISQUALIFICATION <input type="checkbox"/> 1. Alcohol abuse <input type="checkbox"/> 2. Drug abuse <input type="checkbox"/> 3. Negligence/delinquency in duty performance <input type="checkbox"/> 4. Court-martial/civilian convictions <input type="checkbox"/> 5. Physical/mental condition <input type="checkbox"/> 6. Poor attitude/lack of motivation <input type="checkbox"/> 7. Other (Explain in Block 50)
49. PERSON IS DISQUALIFIED FROM THE SUBJECT POSITION/DUTIES <input type="checkbox"/>		
50. RATIONALE		
51. PERSON WAS NOTIFIED OF DISQUALIFICATION ON _____ by _____		
DATE (YYYYMMDD)		METHOD OF NOTIFICATION
52. NAME OF CERTIFYING OFFICIAL (Last, First, MI)	53. SIGNATURE <small>(SEE NAME)</small>	54. DATE (YYYYMMDD)
55. NAME OF REVIEWING OFFICIAL (Last, First, MI)	56. SIGNATURE <small>(SEE NAME)</small>	57. DATE (YYYYMMDD)

Appendix U

Operating Civilian or Privately Owned Radio Controlled (RC) Model Aircraft/Drones/Small Unmanned Aircraft Systems (UASs) on Fort Liberty

1. General.

a. This app provides guidance on the definition, designation and prohibited actions concerning the use of civilian or privately owned Radio Controlled (RC) Model Aircraft / Drones / Small Unmanned Aircraft Systems (UASs) on Fort Liberty.

b. This app is applicable to all persons or entities residing, employed / working, and or visiting Fort Liberty.

2. References.

a. Memorandum, Secretary of the Army, Washington, D.C.; Subject: Army Policy for Unmanned Aircraft on Army Installations, 1 August 2017.


b. Federal Aviation Administration (FAA) / Department of Defense (DoD Joint Standing Operating Procedures (JSOP) for Unmanned Aircraft Systems Specific Special Security Instructions (SSI), 7 April 2017.

c. Title 14, Code of Federal Regulations (14 CFR) § 99.7 (Special Security Instructions and Temporary Flight Restrictions), 20 May 2004.

3. Prohibited actions. The use of civilian or privately owned Radio Controlled (RC) Model Aircraft / Drones / Small Unmanned Aircraft Systems (UASs) on Fort Liberty is consistent with Federal, state, and local UAS laws and regulations, to include FAA designated SSI areas. Fort Liberty Camp MacKall SAAF, and PAAF are considered SSI areas and all drone flight operations are prohibited within the airspace of Fort Liberty and Camp MacKall.

4. Waivers. All waivers concerning the use of civilian or privately owned Radio Controlled (RC) Model Aircraft / Drones / Small Unmanned Aircraft Systems (UASs) on Fort Liberty will be submitted to the Air Traffic Branch, Airfield Division, Directorate of Plans, Training, Mobilization, and Security (DPTMS) at 910-396-7724.

**Appendix V
Duty Appointment Example**

	LETTERHEAD
OFFICE SYMBOL	Date
MEMORANDUM FOR	
SUBJECT: Appointment of (Topic)	
<ol style="list-style-type: none">1. (Reference), effective immediately (Rank/ Last Name/ First Name) is appointed as the (Duty Position). I validate that he/she demonstrates trustworthiness and reliability in carrying out the responsibilities inherent in performing as the (Duty Position).2. A copy of this appointment document will accompany all documentation where you exercise your authority.3. You may not further delegate this authority. This authority may be canceled or withdrawn at any time. Upon my leaving the organization, this delegation is subject to review by the new issuing authority. This authority is automatically canceled upon your retirement, change of duties, or change of position.4. Point of contact is (Rank), (Name), (Position), at (Contact number(s)) or (e-mail).	
Signature Block	
CF: Individual Command	

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

AFSBN

Army Field Support Brigade

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

App

appendix

AROC

Arms Room Operations Course

ASL

authorized stockage list

Glossary - Continued

ASP

ammunition supply point

AT/FP

antiterrorism/force protection

AWOL

absent without leave

BDE

Brigade

BMS

Balance magnetic switch

BN

Battalion

BTRY

Battery

CAC

common access card

CAT

category

CBRNE

chemical, biological, radiological, nuclear and explosive

CCTV

closed-circuit television

CDR

Commander

CCIR

Commanders Critical Information Requirements

Chap

chapter

CoC

chain of command

COMSEC

communications security

Co

company

CP

crime prevention

Glossary - Continued

COTS

commercial off-the-shelf

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

Glossary - Continued

DPW

Directorate of Public Works

DRC

Directorate Readiness Center

DWI

driving while intoxicated

EOD

explosive ordnance disposal

ETS

expiration term of service

FASP

field ammunition supply point

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

GCSS

Global Combat Support System

GRP

group

GS

General Schedule

GSA

General Service Administration

HC

host commander

HQDA

Headquarters Department of the Army

Glossary - Continued

HRT

high risk target

HSP

high security padlock

HVASC

High-Value Asset Security Cage

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

IPSS

Installation Physical Security Survey

IRP

Individual Reliability Program

Glossary - Continued

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

Glossary – Continued

OIC

officer in charge

PACS

Physical Security Access Control System

PAO

Public Affairs Officer

PBO

Property Book Officer

Para

paragraph

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

Glossary - Continued

PSCPO

Physical Security Crime Prevention 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

Glossary - Continued

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

United 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 Liberty, NC relating to vehicle and personnel screening, ID documents, vehicle registration, long term access control card, and temporary passes in IAW AR 190-13, chap 8.

Glossary - Continued

Motor Pool

A group of motored vehicles used as needed by different organizations/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/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 (1) or more component medical Note Q or R items.

Note Q Controlled Medical Items

All standard drug items identified as medical 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 medical 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 U.S. 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.