Department of the Army
Headquarters, United States Army
Maneuver Support Center of Excellence
Fort Leonard Wood, Missouri 65473-5000

FLW Regulation 190-13

3 June 2020

Military Police

FORT LEONARD WOOD PHYSICAL SECURITY PROGRAM

FOR THE COMMANDER

OFFICIAL:

DAVID A. CALDWELL
COL, GS
Chief of Staff

JESSE J. FRENCH
Director, Garrison Human Resources

History. This publication has major revisions and incorporates Fort Leonard Wood (FLW) Reg 190-7 dated 21 Jul 2015 and FLW Supplement 1 to AR 190-13, 22 July 1997.

Summary. This regulation establishes the philosophy, policy, format, guidance, and standardized procedures for the planning, coordination, and execution of the FLW installation's Physical Security Program.

Applicability. This regulation is applicable to all persons who deal directly or indirectly with the Physical Security Program on FLW.

Supplementation. Furth supplementation of this regulation is prohibited unless specifically approved by the Headquarters, US Army Maneuver Support Center of Excellence and FLW.

Proponent. The proponent agency for this regulation is the Directorate of Emergency Services (DES).

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Forms) to Commander, MSCoE, ATTN: IMLD-ESP-S, Fort Leonard Wood, MO 65473-5600.

Distribution. Electronic medium only and posted on the FLW Web site.

*This regulation supersedes FLW Supplement 1 to AR 190-13, 22 July 1997, and FLW Reg 190-7, 21 Jul 2015.

Summary of Changes
To
FLW Reg 190-13, Fort Leonard Wood Physical Security Program and FLW Reg 190-7, Installation Access Control.

FLW Supplement 1 to AR 190-13, 22 July 1997, has undergone major revisions.

- Changes from a FLW Supplement 1 to AR 190-13, to FLW Reg190-13.
- Consolidated FLW Suppl 1 to AR 190-13 and FLW Reg 190-7 into one regulation.
- Incorporates changes to align with AR 190-13, 27 June 2019.
- Chapter 1 added to introduce the regulation to the reader and to establish Staffing responsibilities.
- Chapter 2 added to establish specific Policy.
- Chapter 3 added to define and explain Personnel requirements.
- Chapter 4 added to define and explain Restricted Areas.
- Chapter 5 added and incorporates FLW Reg 190-7 to align with AR 190-13.
- Chapter 6 added to explain requirements and procurement of Physical Security Equipment and Intrusion Detection Systems.
- Chapter 7 added to establish a Crime Prevention program.
- Appendix A changes to References.
- Appendix B added a sample FLW Form 1907 from FLW Reg 190-7.

Chapter 1
INTRODUCTION

The key to the successful execution of military and administrative operations is the continuous protection of assets required for present and future use.

1-1. Purpose

This regulation provides policy, format, and guidance for Fort Leonard Wood (FLW) Physical Security Program not clarified or included in other publications. This regulation does not eliminate the requirements of other publications for developing and maintaining a practical, economical and effective Physical Security Program.

1-2. References

All required publications, and referenced forms within this regulation are listed in Appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

Section I. Responsibilities

1-4. Senior Commander

The Senior Commander will appoint an Installation Physical Security Officer (IPSO) in writing who will report to the Director, of Emergency Services (DES) Garrison Commander on all physical security matters.

1-5. Garrison Commander

a. Ensure, at a minimum, access control is conducted at all operational Installation Access Control Points (IACPs). Provides a level of security at IACPs based on current threats to FLW or the surrounding area of responsibility (AOR) to protect against trespassing, terrorism, sabotage, theft, arson, and/or criminal activity that may pose a threat to health and safety on the installation.

b. Establish and maintain a practical physical or automated access control system or a combination of both to identify and control personnel, vehicles, material, and equipment entering and departing FLW.

c. Allocate the necessary resources to enforce established installation access control measures.

d. Maintain a visitor control program for non-Department of Defense (DOD) affiliated individuals requesting access to enter FLW. At the direction of the Senior Commander determine special event status as to whether background screening is waived on visitors entering FLW for events sponsored by FLW organizations.

e. At the direction of the Senior Commander, serve as the waiver authority to review and determine requests for unescorted access waivers of individuals denied access. Enforce the removal of, or deny access to, persons who threaten the order, security, discipline or health and safety on the installation.

f. Designate restricted areas on FLW, in writing, for which commanders or directors will establish specific access control measures.

1-6. Commanders and Directors

Major subordinate commanders, activity directors/chiefs, separate staff sections and commanders of units, detachments, and tenant activities, will provide internal security for units, facilities, and material located within their assigned areas. Specific responsibilities include:

a. Appoint a Physical Security Officer or Noncommissioned Officer in writing.

b. Operation of a unit interior guard as assigned in accordance with FLW Guard Force Plan. Commanders of military units will provide support as tasked for increased levels of installation access control in accordance with (IAW) the current FLW Emergency Guard Force Plan.

c. Maintain a copy of the last Physical Security Inspection reports on file within the unit headquarters and each unit for 5 years.

d. Submit a listing of all mission essential vulnerable areas (MEVAs) within the command/directorate to the IPSO no later than 1 April of each calendar year. A listing of areas that will be classified as MEVAs is contained in AR 190-13, The Army Physical Security Program Chapter 2.

e. Coordinate all security related renovations, new construction, or changes in the security posture provided to buildings or areas with the IPSO.

f. Establish and maintain an adequate current physical Security Plan/Standard Operating Procedures (SOP) (see Chapter 2) for all assigned areas of responsibility and/or buildings to provide guidance for the protection of Government property and equipment.

g. Establish, in writing, access control procedures for restricted areas as part of Physical Security Pans/ SOPs within their scope of responsibility IAW AR 190-13 and this regulation.

h. Appoint in writing unit/organization sponsoring authorities/point of contact (POCs), responsible for validating access requests for contractors, vendors, service providers or visitors pertaining to their organizational requirements or events.

i. Review family care plan documents, validate requests to grant installation access to family care providers, and ensure proper vetting of these individuals IAW this regulation.

j. Establish at the direction of the Senior Commander unit/activity procedures to ensure all personnel register vehicles IAW AR 190-5, Motor Vehicle Traffic Supervision and this regulation.

k. Provide access control information and requirements in accordance with this regulation to visitors attending unit or organization sponsored special events such as use of the Waynesville St. Robert Regional Airport at Forney Field, InterContinental Hotel Group (IHG) hotels, escorted versus unescorted access, the Real ID Act of 2005, and access by foreign nationals.

1-7 Director, Emergency Services

a. Be the proponent for Physical Security Programs on FLW.

b. Develop local installation access control requirements IAW applicable DoD and Army directives.

c. Control security forces and operations at all IACPs.

d. At the direction of the Senior Commander develop local vehicle registration requirements IAW AR 190-5.

1-8. Installation Physical Security Officer

The IPSO will exercise staff supervision over the Installation's Physical Security Program. Specific assigned duties include:

a. Establish and implement physical security directives as approved by the Senior Commander.

b. Plan and provide physical security assistance, such as physical security work order ratings, aiding in the development of Physical Security/Crime Prevention Plans and standard operating procedures.

c. When requested furnish recommendations and reports to the Senior Commander on all matters related to Physical Security Programs.

d. Schedule periodic Physical Security Surveys of the installation to ensure compliance with applicable directives and provide assistance in resolving physical security related findings.

e. Provide investigating agencies with Physical Security Inspection results surrounding loss, damage, or destruction of sensitive and non-sensitive Government property.

f. Coordinate with the Director of Plans, Training, and Mobilization (DPTM) for selection of sites and facilities requiring additional physical security measures and the determination of urgency for establishing additional protection in various situations.

g. Coordinate military police activities to reinforce physical security efforts of units and activities.

h. Annually review the Installation Physical Security Plan, MEVA list, restricted area list and coordinate with commanders and directors to update as appropriate.

i. Develop and implement access control SOPs for all IACPs based on all Force Protection Condition (FPCON) levels IAW applicable DoD and Army directives and this regulation.

j. Manage installation access control, security forces and operations at all IACPs.

k. Ensure that all arriving airport passengers, to include airport employees, are vetted via National Crime Information Center (NCIC) Interstate Identification Index (III) and processed IAW this regulation prior to allowing access to FLW from the airport.

l. Manage and implement FLW vehicle registration procedures, at the direction of the Senior Commander.

m. Manage and maintain the Visitor Control Center (VCC) and ensure VCC personnel adhere to the requirements of DoD directives, Army regulations and this regulation.

n. Coordinate with unit commanders, when a family care plan is executed within their command, and ensure the care giver is properly vetted IAW this regulation prior to allowing access on to the installation.

o. Review, determine the validity, and approve or disapprove all pass requests for contractors, vendors, or visitors with no organizational sponsor availability, installation thoroughfare requests, and requests for 24 hour 7 day a week access to FLW.

1-9. Director, Network Enterprise Center (NEC)

Provide for all required communication/data lines dedicated solely for Intrusion Detection System (IDS) and communication functions at IACPs IAW command, control, communications, computers, and information management (C4IM) service catalog and service level agreement policy.

1-10. Public Affairs Office (PAO)

a. Establish and coordinate with the FLW legal offices' written procedures/rules for non-commercial imaging (Family member photography/video) and commercial imaging of events (graduations or weddings) on FLW.

b. Be the single POC for sponsorship of public or private non-DOD affiliated media personnel.

c. Escort (by qualified PAO personnel) all authorized media representatives from entry to exit while on FLW. Non-DOD affiliated members of the media will not be allowed unescorted access to FLW.

d. Facilitate the dissemination of information to all stakeholders, tenants, and surrounding communities regarding changes to access control policy.

1-11. Directorate of Plans, Training, Mobilization, and Security (DPTMS)

a. Review all special event staffing papers waiving background screening requirements for visitors entering the Installation.

b. Develop and provide a risk assessment for all special events staffed to the Garrison Commander for approval.

1-12. Military and DOD Personnel

a. All military, and DOD Civilian/contractor personnel are responsible for taking reasonable measures to secure sensitive government materials or Army property within the immediate area of their authority even though guards may be assigned to their activity. This guard protection is external and its purpose is to prevent intrusion after duty hours.

b. Provide current valid identity documents and be prepared to provide required vehicle documentation when requesting access to FLW.

c. Understand that access to FLW carries implied requirements to abide by established laws and regulations. All persons and vehicles are subject to safety and security inspections at any time while entering or on FLW.

Chapter 2
POLICY

2-1. Waivers and Exceptions

a. Waivers and Exceptions will be requested as a last effort, after all attempts at physical or

procedural mitigation measures have been exhausted to meet regulatory requirements. They will not be used to reduce or eliminate minimum regulatory security requirements. Compensatory measures will be used during interim periods.

b. All requests for waiver or exception will be submitted IAW AR 190-13, chapter 2. Coordinate requests with proposed compensatory measures through the IPSO.

c. When a deficiency is identified that is correctable within 60 days do not submit a request for waiver. Compensatory security measures will be taken and specified in writing by the responsible commander/director during this interim period.

2-2. Physical Security Plan Considerations

Physical Security Plans will be established for all units and activities.

a. Develop access control procedures for unit areas and facilities to preclude the entry of unauthorized personnel. These plans will include a unit standard operating procedures for courtesy patrols, interior guards, charge of quarters, barracks guard and/or duty personnel which will contain specific instructions defining personnel authorized to enter particular unit areas and facilities and disposition of unauthorized person.

b. Coordinate all Physical Security Plans through the IPSO annually for review and inclusion as annexes into the Installation Physical Security Plan. Approved Plans will be validated with a stamp/date issued from the Security Operations Division.

2-3. Physical Security Plan/SOP Format

The format for establishing Physical Security Plans is found in AR 190-13, Appendix C. All applicable areas will be addressed. The following additional areas will be included and/or specifically expounded upon.

a. Security Forces. Include general instructions which would apply to all security force/guard personnel. Detailed instructions such as Special Orders and standard operating procedures should be attached as annexes.

b. Key Control and Accountability. Key and lock control programs will be IAW applicable Army and FLW regulations listed below. Automated key control system procedures will be IAW AR 190-51, Security of Unclassified Army Resources (Sensitive and Nonsensitive). Key and lock control procedures may be a separate annex to the Physical Security Plan.

(1) Arms, Ammunition, and Explosives (AA&E) room keys and lock. Will be established IAW AR 190-11, and FLW Reg 190-11 Physical Security of Arms, Ammunition and Explosives.

(2) Non-arms room (Administrative keys). Will be established IAW AR 190-51, Appendix D.

c. Emergency Actions. Indicate emergency actions of a general application.

(1) Actions during a kidnapping and/or hostage situation.

(2) Actions upon receipt of a bomb threat.

(3) Contingency planning will include security response and work curtailment or shift procedures for natural disasters, man-made emergencies and increased threats from terrorist or criminal elements.

d. AA&E SOP will be attached as an annex to unit/activity Physical Security Plans.

2-4. Physical Security Inspections

Physical Security Inspections are tools for commanders/directors to assess physical protective measures and procedures, and make informed decisions on corrective action(s) to eliminate or mitigate identified weaknesses within the unit/activity Physical Security Program. Physical Security Inspections are conducted IAW AR 190-13, paragraph 2-15.

a. Announced and unannounced inspections are conducted and inspectors will, when possible, review unit/activity schedules prior to any inspection in an effort to minimize the impact on unit operations.

b. All government/Army property or assets on FLW or within the AOR, listed in an AR 190-series will be inspected, IAW applicable regulations, policies, directives, and SOPs to assess compliance with required physical security protective and procedural measures.

c. Pre-occupancy inspections will be conducted for all new AA&E facilities or when units are scheduled to move weapons into an existing AA&E facility. A follow-on initial inspection will be conducted within 30 days after occupancy. A post-occupancy inspection will be conducted when these areas are closed.

d. Initial inspections will be conducted for all areas when a unit or activity is activated or when no record of a prior inspection exists.

e. Re-inspections will be conducted for all areas receiving a not-adequate rating. These re-inspections will be conducted in coordination with unit commanders 6 months after the last inspection.

2-5. Corrective Action Report

A Corrective Action Report (memorandum) will be completed for each Physical Security Inspector/Inspection (PSI), with a not-adequate rating. The report will address at least the following:

a. Restate each deficiency listed on the PSI report.

b. List the corrective action for each deficiency. Explain any submitted work orders, Command Policy Letters, SOPs, or other actions taken to correct or compensate for security shortfalls.

c. The corrective action report will be forwarded through the unit's next higher command (Brigade or equivalent) and then to the Installation Physical Security Office, ATTN: IMLD-ESP-S.

d. Corrective Action Memorandum will be signed by the unit/activity Commander or Director. Reports will be submitted by the suspense date assigned which is 30 days from the date of signatures on the PSI report. Maintain on file until the next Physical Security Inspection is conducted.

Chapter 3
PERSONNEL

3-1. Physical Security Officer Appointments

a. Physical Security Officers will be appointed in writing.

b. Brigade/Battalion/Directorate level PSOs will be Sergeant First Class/E7 or above; DOD Civilian equivalent or above.

c. Company/Detachment levels will be Staff Sergeant/E6 or above; DOD Civilian equivalent or above.

d. PSO appointees will demonstrate a working knowledge of physical security through one of the following qualifications below and will complete all requirements in AR 190-13, chapter 3-1b(1).

(1) Documented prior experience managing a Physical Security Program. (S2, PSO, Key Control Officer)

(2) Formal documented physical security operations training. (FLW, DES, Security Operations Division Physical Security Class)

3-2. Physical Security Inspectors and Credentials

a. Physical security inspectors will be selected by the IPSO IAW AR 190-13, Chapter 3.

b. PSI credentials (DA Form 4261 and 4261-1) will be controlled and awarded by the Installation Physical Security Officer. The same form issued by any other agency will not be valid or recognized on FLW.

Chapter 4
RESTRICTED AREAS

4-1. General

FLW Army Installation, as defined by established physical man-made and natural boundaries, is designated as a restricted area. See the Installation Physical Security Plan, annex S to FLW, Emergency Management Operations Plan for a current listing of designated restricted areas.

4-2. Requirements

a. Unless necessary for security purposes to conceal an area, designated areas will be posted with signs that identify the site as a restricted area. Signs will be worded and positioned IAW AR 190-13, Chapter 6.

b. The IPSO will be notified in writing of all proposed changes to restricted areas that change building or room structural compositions, any proposed installation or movement of IDS/physical security equipment (PSE) or repurposing of the area.

c. When AA&E storage areas are empty/inactive all unit/user requirements IAW AR 190-11/FLW Reg 190-11 for IDS testing, key and lock control, and any other requirements dealing with the structure will be maintained as if the area was active. AA&E areas approved by the IPSO for repurposing may be exempt from these requirements.

d. Commercial imaging surveillance by photography or video recording is prohibited on FLW. Title 18 USC 795 prohibits photographing and sketching defense installations without permission. Commercial surveillance vehicles will be denied access to FLW unless prior coordination is established and they are escorted by a PAO representative.

Chapter 5
FORT LEONARD WOOD ACCESS CONTROL

5-1. General

Minimum requirements for controlling access to Army installations are outlined in AR 190-13, Chapter 6 & 8, this regulation and Installation Access Control Point (IACP) SOP.

5-2. Policy

The DES is the authority for granting or denying access to FLW. The DES Director (Provost Marshal); Deputy Director; and Chief, Security Operations may implement exceptions to this regulation, if a situation necessitates an exception to accomplish or improve installation access control, while not violating the spirit of this regulation or creating a security or force protection vulnerability. Persons, vehicles, materials, and equipment may be authorized access through designated IACPs based on FPCON, a valid access requirement (as noted in paragraph 5-3), a DOD-affiliated sponsorship, current state vehicle registration, proof of current vehicle insurance, current state-issued vehicle operator license meeting the Real ID Act of 2005, and assessment of an authorized FLW identification (ID) document. (See Department of Homeland Security (DHS) website (https://www.dhs.gov/real-id) for more information on the Real ID Act of 2005)

a. All pedestrians (walking in) or individuals riding in or on, any mode of transportation, will have their ID document verified prior to access authorization.

b. Prior to installation access, all person(s) age 18 and older will provide a FLW recognized identity document for vetting and validation. The method of verification of these documents may be physical, automated, or a combination of both.

c. Children, reasonably evident to be under the age of 18, are not required to produce an identity document if they are with a parent or an adult cleared to enter the installation.

d. Personnel having a DOD ID document or a valid FLW pass issued to them will use this card/document when accessing FLW. Personnel possessing valid DOD ID cards are not required to routinely undergo the vetting process as it is part of the identity-proofing standards prior to issue of the DOD ID card. All documents are still subject to current FPCON random antiterrorism measure (RAM) and vetting against the access control system.

e. See paragraph 5-11 for special event requirements.

f. Information on all presented identity documents are subject, at a minimum, to a cross referencing through the NCIC III, State Crime Information Center, available United States Government (USG) information databases, and/or the access control system denied access list, driving suspension list, restricted driving list, and the FLW debarment list.

g. Non-DOD affiliated personnel requiring access will be sponsored by an authorized DOD-credentialed individual associated with FLW or a FLW-DOD organization, possessing sponsorship authority as specified in paragraph 5-6. Sponsorship privileges may be suspended as directed by the Senior Commander or designated representative based on current FPCON levels, extenuating circumstances, or a violation of sponsorship requirements established within this regulation.

h. Non Common Access Card (CAC)-holder contractors and vendors.

(1) Contractors and vendors requiring physical access to a single Army installation or facility, but who do not require access to a DOD computer network, will have a Government-employee sponsor to provide the contractual agreement with a cover memorandum signed by a verifying officer vouching for the need for long-term access to the installation. The expiration date of the issued card will be the end

date of the contract or visit, or the expiration date of the sponsor's access control card, whichever occurs first. Sponsors will be held responsible for notifying the DES (or appropriate local installation access issuing office) of terminated contract employees and for turn in of expired or revoked ID.

(2) Contractors will be processed through the Contractor Verification System for issuance of a CAC, if physical access to multiple Army installations and/or access to a DOD computer network is required.

(3) Non CAC-eligible contractors will be issued an access ID that will only be used for physical access onto the installation.

(4) FLW associated DOD organizations and activities needing to establish recurring access authorization for non-DOD personnel that do not meet CAC eligibility requirements, or during an interim period, will implement the requirements of this regulation for sponsoring these individuals. These requirements will be included in the contracting process for contracts written on or off FLW. Contractor and all associated subcontractors' employees shall comply with applicable installation and facility access and local security policies and procedures provided by the government representative. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the Installation Provost Marshal Office, DES, or Security Office. The requesting contractor may submit their request for an installation pass to their sponsor using the pass application portal. A valid DOD sponsor may be either the contracting office representative (COR), contracting office technical representative (COTR), or contracting officer (KO) if neither is appointed. Contractor workforce must comply with all personal identity verification requirements as directed by the Real ID Act of 2005; DOD; Headquarters, Department of the Army (HQDA); and/or local policy. In addition to the changes otherwise authorized by the changes clause of a contract should the FPCON at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

i. Denial of entry. Fitness for unescorted or escorted access will be determined by an analysis of information obtained through authoritative government data sources. At a minimum, a query of the NCIC III and the Terrorist Screening Database is conducted to determine if the person requesting unescorted access presents a potential threat to the good order, discipline, or health and safety on the installation. Such derogatory information includes, but is not limited to, the following:

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

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

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

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

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

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

(7) The individual is a registered sex offender.

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

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

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

(11) Failure to provide adequate or valid identity documentation, Real ID Act compliant driver's license, proof of valid vehicle registration, and insurance.

(12) Failure to prove a legitimate need for access to FLW.

(13) Increased FPCON levels for which entry may be restricted to mission essential persons only.

(14) Failure to meet DOD sponsorship or escort requirements specified in this regulation.

(15) Failure to comply with random safety and security inspections.

(16) Attempting to access FLW with unregistered firearms or in possession of prohibited items as outlined in AR 190-11 and FLW Reg 190-11.

(17) Individuals identified by the Immigration and Customs Enforcement (ICE) database as residing in the US in a non-legal status. Persons in this status are not authorized unescorted or escorted access. A waiver may be requested upon attaining legal status.

j. In the event that an individual is denied unescorted access to the installation based upon derogatory information obtained from the NCIC III check, the DOD POC/sponsor and access requestor will be informed of the ability to request a waiver. The instructions will direct the access requestor to—

(1) Provide a completed FLW Form 1907 (Request for Access Waiver Packet Checklist) (sample at appendix B) through the DOD POC/sponsor who is responsible for submitting the waiver request to the Senior Commander or designated waiver authority representative.

(2) Provide a current certified copy of their complete criminal history, to include all arrests and convictions from all States in which they have criminal history.

(3) Provide a letter of support from their DOD POC/sponsor. The letter must indicate that the sponsor requests that the individual be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visit. If the contractor employee is terminated, unescorted access to the installation is no longer authorized. The sponsor must inform the VCC for revocation of the unescorted access.

(4) In the personal waiver request letter, all offenses and arrests must be listed, along with an explanation why the conduct should not result in denial of unescorted access to include any impact on the individual and/or mission of FLW as result of the denial. Other factors to be addressed in the waiver request letter include-

(a) Nature and seriousness of the conduct.

(b) Specific circumstances surrounding the conduct.

(c) Length of time elapsed since the conduct.

(d) Age at the time of the incident or conduct.

(e) Provide a letter of reference or recommendation from employer if applicable.

(f) Provide proof of efforts toward rehabilitation.

5-3. Valid and non-valid access determinations

Persons requesting to enter FLW must have a valid purpose to gain escorted or unescorted access to the installation. The determination for some circumstances may require a case-by-case decision as directed by the Senior Commander or designated representative and FPCON. To assist with this determination minimum guidelines are listed below.

a. Unescorted personnel. A valid purpose to have unescorted access to FLW may include but is not limited to the following accepted access needs:

(1) Individuals—

(a) Employed as a contractor, vendor, and service providers to the installation (such as food delivery, taxi driver, or tow truck drivers).

(b) Visiting the Army museums.

(c) Using specifically authorized events or facilities by Morale, Welfare, and Recreation (MWR) facilities such as the golf course or bowling center.

(d) Using FLW as a thoroughfare on a recurring basis.

(e) Hunting and fishing on FLW.

(f) Validated use of the Waynesville St. Robert Regional airport and Forney Army airfield or IHG hotels.

(g) Individuals not CAC eligible with an approved housing lease on FLW. These individuals are not authorized sponsorship or escort privileges on FLW. Guests of these individuals may receive a pass for up to 72 hours for the purpose of visiting them at their leased housing. The person with the housing lease must physically meet the guest at the Visitor Center to vouch for the visitor and accompany them to their leased housing. Guests must meet all other access requirements of this regulation before access will be granted.

(h) Visitors attending FLW sponsored special events may be granted unescorted access as directed by the Senior Commander. Specific guidance for access control procedures at FLW sponsored events is IAW AR 190-13 and paragraph 5-11 based on the current FPCON and risk assessment.

(i) Individuals affiliated with the Department of the Army (DA) Survivors Outreach Services (SOS) Program are authorized unescorted access to FLW. The date the NCIC III check is conducted must be typed on the DA Form 1602 (Civilian Identification) when issued. Gold Star members may also be issued an access card/pass not to exceed 3 years before expiration.

(j) Official foreign visitors such as Foreign Liaison Officers, Foreign Exchange Personnel, and Cooperative Program Personnel subject to the provisions of AR 380-10, Foreign Disclosure and Contacts With Foreign Representative, and assigned on orders to FLW will be granted unescorted visitor status and may sponsor and escort within the requirements of this regulation. The foreign visit system confirmation module will be used to confirm the proposed official visit to FLW. Foreign visitors subject to the provisions of AR 12-15, Joint Security Cooperation Education and Training do not have sponsorship or escort privileges. A check of NCIC III and Terrorist Screening Database records will not be conducted for these official foreign visitors. For additional information or guidance contact the FLW Foreign Disclosure Officer.

(k) When emergency response vehicles/personnel enter under emergency conditions these vehicles will be delayed the minimal amount of time to verify operator information for security purposes. These procedures also apply for personnel transported in a privately owned vehicle (POV) under emergency conditions. When emergency vehicles/personnel are requesting unescorted access for nonemergency condition, the requirements for validated access as specified in this regulation will apply and vehicle/occupants are subject to RAM inspection.

(l) Clergy sponsored by the Installation Chaplain's Services that do not meet CAC eligibility requirements may receive an unescorted pass for "official business only."

(m) Students or employees affiliated with colleges on FLW that do not meet CAC eligibility requirements may receive an unescorted access card or temporary pass based upon employment and/or for the semester(s) they are scheduled to attend classes, not to exceed (NTE) the term.

(n) Directorate of Family Morale, Welfare, and Recreation (DFMWR) Non-appropriated Funds (NAF) flex employees that do not meet CAC eligibility requirements may receive an unescorted pass for "official business only."

(o) Moving and freight companies approved and sponsored by the FLW, Logistic Readiness Center (LRC) Transportation Division that do not meet CAC eligibility requirements may receive unescorted access passes for "official business only" for a period NTE length of contract or 12 months whichever is shorter.

(p) Waynesville R-6 School District faculty and parents of nonmilitary affiliated children attending a Waynesville R-6 school facility located on FLW that do not meet CAC eligibility requirements may be sponsored by the MWR School Liaison's sponsoring authority and issued an unescorted pass for the current school year.

(q) Veteran's health identification card (VHIC) cardholders with an approved General Leonard Wood Army Community Hospital (GLWACH) medical appointment may be granted unescorted access IAW this regulation after completion of an NCIC III check and FLW pass issued.

(r) Foreign national spouses of FLW, DOD Civilian employees not eligible to receive a DOD ID card may be sponsored by their DOD Civilian spouse for an unescorted FLW pass not to exceed 12 months. Person(s) must be legally residing in the US. These persons do not have sponsorship or escort privileges. These passes will terminate immediately upon the termination of employment of the FLW DOD Civilian.

(s) DoD retiree(s), or DoD ID card holders accessing the Installation for purposes of commercial or business gain or for the furtherance of a contract, must be screened and receive the appropriate FLW pass. When accessing the Installation for privilege purposes such as personal use of the Commissary, Post Exchange (PX), MWR facilities, or activities that are not commercial/business/contracted then they must use their issued DoD ID card.

b. Escorted personnel. The following examples are not valid reasons for unescorted access but may be valid when escorted by a DOD ID cardholder.

(1) Patronage of eating establishments (such as Burger King, Dunkin Donuts, or PX Food Court), shopping at the Army and Air Force Exchange Service (AAFES) retail establishments, use of MWR fitness centers, or general sightseeing outside the scope of Army museums.

(2) Non-DOD affiliated visitors not providing goods and services to the installation but wish access onto FLW. This pertains to all visitors not attending a DOD-sponsored special event but may have a one-time or intermittent request to access FLW with a DOD ID cardholder. Visitors require a DOD sponsor/escort at all times while on FLW, and between the hours of 2100 and 0500 will be signed-in at the gate of entry by the DOD sponsor/escort, have a favorable background screening and issued a FLW pass.

(3) US citizens previously denied unescorted access due to unfavorable background screening results, may be escorted by an authorized DoD ID card holder. The DoD sponsor/escort will sign-in their visitor at the gate of entry and by signature will acknowledge their requirement to escort visitor(s) at all times while on FLW.

(4) Foreign national persons not subject to the provisions of AR 380-10 require DOD sponsorship, background vetting, and escort prior to gaining access and while on FLW.

(5) Creditors, or their repossession agents, requesting access to FLW to recover property based on default of a contract or legal agreement will coordinate through the DES and be escorted by Military Police. The creditor or their agent must present copy of title, contract or legal agreement, and present evidence that the debtor is in default, and agents must present evidence they are working for the creditor.

5-4. FLW recognized DOD access identity documents

a. DOD-identity documents listed in AR 190-13 and below are recognized for unescorted access to FLW without needing NCIC III vetting once the document and individual holder are verified.

b. DD Form 2574 (Armed Forces Exchange Services Identification and Privilege Card).

c. FLW locally produced installation card or pass, designated for unescorted access on the document when issued.

d. FLW Form 1817, (Maneuver Support Center of Excellence Temporary Vehicle Pass), temporary 24-72 hour visitor pass when accompanied by a valid Real ID Act compliant state-issued driver's license for the individual to whom the pass was issued and designated for unescorted access on the document when issued.

5-5. FLW recognized non-DOD access identity documents

The following federal or state-issued identity documents may be used to verify the identity of a requestor prior to the issuance of an access card or visitor pass for unescorted or escorted access as directed by the Senior Commander or designated representative. NCIC III background vetting is required. Issuance is subject to all requirements and restrictions of this regulation. All identity documents or combination of below listed documents must at a minimum provide a photograph and information such as name, date of birth, gender, height, eye color, and address.

a. Authorized United States Citizens Identity Documents.

(1) Valid Real ID Act Compliant state driver's license or ID card (state or territory of the United States).

(2) U.S. Passport (signed and unexpired).

(3) U.S. Coast Guard Merchant Mariner Card.

(4) U.S. Postal Service (PS) non-contractor employee ID cards: PS Form 5140 (Non-Postal Service Contract Employee) and PS Form 4098 (Employee Identification Card).

(5) All forms of U.S. DHS non-contractor government employee ID Cards.

(6) U.S. Government Investigative Services non-contractor ID Card.

(7) Transportation Security Agency, Transportation Worker Identification Credential (TWIC). Foreign nationals with TWIC must meet all vetting, sponsorship, and escort requirements of this regulation.

(8) U.S. Government-issued authenticated federal personal identification verification credentials.

(9) The Veterans Administration Health Identification Card and Veteran Identification Card are valid documents for vetting – but not for access.

b. Authorized Foreign National Identity Documents. (Used to apply for temporary installation pass during special events or sponsored visits, NCIC III vetting required.)

(1) Driver's license issued by a Canadian government authority, provided it contains a photograph and information such as name, date of birth, gender, height, eye color, and address.

(2) Unexpired foreign passport with Form I-551 (Alien Registration Receipt Card) stamp or attached Form I-94 (Arrival-Departure Record) indicating unexpired employment authorization.

(3) Form I-151 (Permanent Resident Card) or Form I-551 (Alien Registration Receipt Card) with photograph.

(4) Unexpired Form I-688 (Temporary Resident Card).

(5) Unexpired Form I-688A (Employment Authorization Card).

(6) Unexpired Form I-327 (Reentry Permit).

(7) Unexpired Form I-571 (Refugee Travel Document).

(8) Unexpired Form I-688B (Employment Authorization Document) issued by DHS that contains a photograph.

5-6. Sponsoring authority

Sponsorship/escort privileges may be suspended as directed by the Senior Commander or designated representative based on current FPCON levels, extenuating circumstances, or a violation of sponsorship/escort requirements established within this regulation. DOD sponsors must be affiliated with FLW to exercise sponsoring or escort authority. All DOD sponsors are validated against DOD databases to ensure they are a current DOD ID cardholder.

a. Uniformed Service members, DOD employees (non-contractors) with a valid CAC, military retirees, or DOD military affiliated spouses with a valid DOD ID card may sponsor visitors onto the installation based on the below restrictions. The number of non-Family member visitors sponsored will not exceed the sponsor's ability to reasonably escort or maintain accountability for those individuals while they are on FLW.

b. DOD sponsors are responsible for validating a requesting individual's need to access FLW and meeting any escort requirements prescribed by this regulation for their visitors at all times while on FLW.

(1) Sponsored visitors (non-DOD ID cardholders) who may require recurring access to FLW may preregister a request for access to FLW via the pass application portal. DOD POC/sponsors may contact the VCC for information on how visitors may access the pass application portal.

(2) DOD sponsors must validate pass application portal requests prior to visitor's arrival. Failure to validate may result in a delay or denial of guest access.

(3) When the pass application portal is not functioning, DOD sponsors will send request via e-mail with digital CAC signature to the VCC <usarmy.leonardwood.usag.mbx.desvisctr@mail.mil> or drop off a signed memorandum in person and show a valid DOD ID card to verify sponsorship authority. Memorandum or email must provide visitor's full name, relationship to sponsor, date of birth (DOB), ID card/document number, from and to visit dates, printed name, and physical or digital signature of DOD sponsor.

c. DOD/DA Civilian employees (non-contractors) may sponsor visitors IAW their assigned duties for example, COR for contracts, subject to current FPCON. When an escort is required, access to the installation will not be granted without a DOD sponsor present.

d. Sponsored contractors, vendors, sub-contractors, service providers, visitors, and international military students assigned to International Student Detachment; do not have sponsorship or escort authority on FLW. DOD ID cardholders that are contractors/vendors that have an active DOD contract or provides a commercial service to FLW do not have sponsorship or escort authority on FLW as it pertains to the execution of that contract or service.

e. NAF, AAFES, Defense Commissary Agency (DeCA) employees when designated by their organization as a DOD-sponsoring authority and in possession of a valid DOD ID card may sponsor/escort visitors onto FLW, subject to current FPCON restrictions.

f. For commercial entities and persons not having a contract or agreement with a FLW organization but having a valid justification for accessing FLW unescorted on a recurring basis, the Installation Physical Security Officer will be the validating official and sponsoring authority. Persons in this category that will require an escort will not be sponsored for a FLW pass or be escorted by the Installation Physical Security Officer.

5-7. Organizational sponsoring authorities

Sponsoring organizations include DOD organizations assigned, attached to, or are a primary resident of the FLW installation.

a. All DOD sponsoring activities/organizations will use an appointment letter signed by the commander or Director to designate individual(s) approved to authenticate and coordinate requests for access for that organization with the VCC. The VCC will maintain this information on file. DOD sponsoring activities/organizations will verify current status of sponsoring authorities with the VCC at a

minimum semi-annually. Appointment letters will be resubmitted annually or upon change of appointment authority within the organization. Organizational sponsorship authority will terminate 12 months from the date of the letter. Appointing authorities must notify the VCC immediately when an organizational sponsoring authority is rescinded.

b. Only DOD-sponsoring authorities on with a valid appointment letter will be authorized to authenticate entry authorization lists and forward these to the VCC for processing.

c. All sponsors must be a non-contractor DOD ID cardholder.

d. Walk-in customers and pass application portal requests for access will be handled by the VCC during normal business hours. Holidays, FPCON restrictions, and network/equipment issues may affect days and hours of operation.

e. VCC personnel will notify sponsoring authorities when passes are ready for pick-up. Visitors must bring their identification documents with them to receive their pass. ID must be Real ID Act compliant. (See DHS website (https://www.dhs.gov/real-id) for more information on the Real ID Act of 2005)

f. DOD POC/sponsors will provide information and guidance to individuals requesting access to FLW IAW with this regulation and will ensure that all information needed to complete a background check is provided. The following information is needed to complete a background check:

(1) DOD POC/sponsor's e-mail.

(2) Visitor's e-mail.

(3) Drivers' license and state.

(4) Beginning date of visit (employment/contract start date).

(5) Ending date of visit (NTE the length of the contract or 1 year, whichever is shortest).

(6) Visitor's last name, first name, middle name and suffix (Sr, Jr, III).

(7) DOB.

(8) Color of hair.

(9) Color of eyes.

(10) DOD-sponsoring organization.

g. Sponsoring organizations are responsible for meeting all escort requirements directed in this regulation.

5-8. Vehicle access

a. Motor vehicles are permitted controlled entry IAW AR 190-5 with a valid vehicle operator's license, current vehicle insurance, and current state registration documents.

b. Access may be denied to vehicles that are obviously defective. Access will be denied when the driver does not possess a valid state driver's license, current vehicle insurance, and current state registration documents or the condition of the driver would result in the unsafe operation of the vehicle.

c. Signs are posted at all authorized IACPs advising personnel that entry to the installation subjects their person and property to safety and security inspections IAW AR 190-13.

5-9. FLW access card and visitor pass

DOD-sponsoring authorities are responsible for submitting requests for pass renewals upon their expiration.

a. Access cards and passes may be issued to personnel not meeting CAC eligibility requirements that are successfully vetted through NCIC III and meet registration requirements of this regulation. Access cards/passes only allow access to the person issued the pass and is valid only for the purpose for which it was issued.

b. Individuals with a valid need for recurring access to FLW for more than 180 days may be issued an access card. Individuals with less than 180 days may be issued a visitor paper pass. All access cards/passes are issued through the VCC. Cards/passes are automatically invalid on the predetermined expiration date.

c. All cards and passes are subject to current FPCON and day/time restrictions. Sponsoring authorities will set individual FPCON restrictions based on the METS (paragraph 5-10 this regulation).

d. Commercial entities employing personnel that do not meet CAC eligibility requirements with a valid licensing/contract agreement may be eligible to receive an access card/pass for the period of the licensing agreement/contract or 12 months whichever is shortest.

e. NCIC III vetted identity documents will be considered vetted for installation access purposes, for a period NTE 12 months. All identity documents are subject to additional vetting processes at IACPs based on the current FPCON.

f. The FLW Form 1817 may be issued from all IACPs to authorized visitors meeting the requirements of this regulation, with a temporary need to access FLW for longer than 24 hours but less than 72 hours. These passes will be honored at all gates when accompanied by the valid photo ID listed on the pass, requirements of the Real ID Act of 2005 will apply. Visitors needing extended passes must report to the VCC with their sponsor during normal operating hours to receive a pass that may extend access authorization longer than 72 hours.

5-10. Mission Essential Tier System (METS)

Based on the scope and nature of an incident, there may be a need to limit traffic flow, restrict access to key facilities, and to prioritize emergency response. The below guidelines will be used to identify personnel deemed mission essential for emergency responses to natural and/or man-made incidents as well as provide the ability to conduct multiple operations to protect the installation during elevated FPCONs.

a. All DOD schools, commands, directorates, and agencies on FLW will identify and designate personnel in writing using the tier system outlined below. Organizations are responsible for informing personnel of their current status and tier they fall under. The maintenance of the list is the responsibility of the organization and will be submitted at a minimum once a quarter or sooner as personnel changes dictate.

b. Lists for Tier 1 through Tier 4 will be kept up to date and submitted to the Antiterrorism Office (ATO) for approval. The AT Office will verify lists and submit to the Installation Operations Center (IOC)/Emergency Operations Center (EOC) and DES Security Operations Division for inclusion on the emergency alert rosters. Final approval for all disagreements with tier placement will be the Garrison Commander.

c. The DES will use the tier system list in conjunction with Installation Access Control Systems for access control during natural and/or man-made emergencies. Personnel listed on Tiers 1 thru 3 may be issued an access card denoting mission essential access at the specified tier.

d. When situations affect the installation, information will be clearly announced utilizing appropriate command channels indicating which tier is to report.

- Tier 1 – Emergency Responders and First Responders (RED). Personnel that work closest to known or suspected hazard and/or in support of life only (for example, police; fire; emergency room; explosive ordnance disposal [EOD]; and chemical, biological, radiological, nuclear, and high-yield explosive [CBRNE]) as needed based on event or hazard.

- Tier 2 – Critical Personnel (YELLOW). Personnel performing a critical function for which there is no backup or alternate but critical to the operations/infrastructure of the installation (for example, EOC/Crisis Action Team (CAT) members, additional caregivers, senior command and control (C2), and infrastructure personnel needed to sustain emergency operations based on event or hazard.

- Tier 3 – Essential Personnel (GREEN). The key group of personnel that ensure continuity of operations for the installation. These positions are cross trained to ensure backups/alternates are available to maintain operations (for example, LRC drivers (as needed), dining facility personnel, drill sergeants, all other commanders, and hospital personnel that directly support caregivers.

- Tier 4 – Snow and ice removal (SNAIR) Essential Personnel.

- Tier 5 – Other Personnel. All other personnel not in above categories needed for normal operations (for example, AAFES/DeCA, admin personnel, instructors, and range personnel).

5-11. Special event access control

Access control procedures for special events (for example, MWR events, 4th of July events, graduations, and concerts) directed by the Senior Commander as open to the public will not sacrifice security for convenience. DOD organizations sponsoring or responsible for special events that may involve an above normal introduction of non-DOD affiliated personnel onto the installation will ensure that appropriate public announcements are provided with the security-related requirements clearly defined. Access control requirements for contractors or vendors participating or supporting special events are not waived and must meet all requirements within this regulation for contractors and vendors.

a. DOD organizations sponsoring or responsible for special events on FLW must submit a FLW Form 1416 (MSCoE Staffing Paper) through the Garrison Commander requesting the event be designated as a special event for access control requirements.

(1) FLW Form 1416 must be submitted through the DPTMS AT Office for inclusion of a risk assessment prior to submission to the Garrison Commander for decision.

(2) FLW Form 1416 must be submitted at a minimum 6 weeks in advance of the event date.

b. During increased FPCONs, units sponsoring a DOD graduation event or special event will provide the VCC with an EAL 10 working days prior to the scheduled event to be entered into the access control system. Visitors entered into the system must present the identity document listed on the submitted EAL when accessing FLW. Visitors not entered into the access control system by the submitted EAL will be processed through the VCC. The requirements of the Real ID Act of 2005 will apply.

c. For other special events (such as MWR events, 4th of July events, and concerts) the Senior Commander will determine the use of physical or automated identification screening or a combination of both, based on the current FPCON.

d. Graduating Soldiers, Marines, Sailors, and Airmen that have foreign national Family member visitors attending family day and/or graduation ceremonies will need to submit for an installation pass 10 working days in advance of the visit date. Foreign nationals in the US with a non-legal status will be denied unescorted or escorted access.

e. Visitor passes may be processed via the pass application portal or e-mailed to the VCC at <usarmy.leonardwood.usag.mbx.desvisctr@mail.mil>. Visitors must include the information required by the pass application portal when requesting a pass. Once applications are submitted via the portal, an e-mail will be sent to the DOD POC/sponsor's e-mail address requesting approval. Upon approval by the DOD POC/sponsor, an e-mail will be sent to the applicant informing them that their pass was approved and that the application will be registered at the VCC where it will be processed for NCIC III and U.S. ICE background screening. Upon process completion, a response will be sent to the DOD POC/sponsor via an e-mail from the VCC stating when the applicant may pick up the pass (beginning date of visit).

f. Information required to complete a pass request:

(1) DOD POC/sponsor's e-mail (graduating student or unit sponsoring authority).

(2) Visitor's e-mail.

(3) Drivers' license and state or passport number and country,

(4) Beginning date of visit.

(5) Ending date of visit.

(6) Last name, first name, middle name.

(7) DOB.

(8) Color of hair.

(9) Color of eyes.

(10) Sponsoring organization (graduating unit).

(11) Reason for visit/access to FLW is requested.

g. Visitors must bring their personal identification documents with them to the VCC to be issued a pass prior to entering the installation. Passes will not exceed 72 hours in visit length.

h. Graduating unit representatives may contact the Security Operations Division to obtain guidance on submitting applications for visitors unable to access the pass application portal or follow paragraph e., above.

i. U.S. Citizens attending student family days and graduations may be authorized temporary unescorted access on the dates of those events without a pass. For these personnel attending special events and activities, NCIC III screening may be waived. Person(s) requesting access must possess a valid, current Real ID Act compliant state-issued driver's license or identification card. Unescorted access is subject to change based on FPCON levels and as directed by the Senior Commander. Visitors wishing to gain unescorted access during the hours of 2100 – 0500 will require DoD ID cardholder sponsorship and a FLW Form 1817.

5-12. Special event privately owned vehicle (POV) access

Visitors requesting unescorted access for the purpose of attending an installation-sponsored event may be authorized access by POV based on FPCON level and as directed by the Senior Commander. As directed by the Senior Commander, an access control system screening may be used as a RAM.

a. Event traffic for visitors not in possession of an installation pass may be directed to and processed through a designated IACP or specified IACP lane. All other routine entry traffic will be directed to use other available IACPs for a specified time frame. This will enable security personnel to focus compensatory security efforts on special event traffic and maximize routine traffic entry at other IACPs.

b. Vehicles may be subject to safety and security inspection based on current FPCON and RAM. At a minimum, security personnel will visually inspect the passenger and non-passenger interior of all vehicles and other measures as directed.

5-13. (Punitive) FLW access policy violations

a. Issued FLW cards/passes are not authorized for transfer among individuals or vehicles. Unauthorized alteration and/or to produce a facsimile and improper use of a FLW card/pass may subject the holder to denial of installation access (debarment) or revocation of access privileges.

b. DOD POC/sponsors that knowingly sponsor an individual(s) that is debarred from accessing FLW, is known to have an active criminal warrant, or does not have a valid reason for accessing FLW may be subject to removal of sponsorship authority and administrative action as directed by the Senior Commander.

c. DOD POC/sponsors failing to comply with their escort responsibilities will lose the privilege to sponsor or escort individuals on FLW. For first offenses privileges are revoked for a period of up to 30 days, 120 days for second offense and 1 year for the third offense.

d. Persons attempting further unescorted access to FLW after being denied unescorted access that have not received an approved unescorted access waiver may be subject to criminal prosecution.

e. Foreign nationals with legal status in the US but without DOD sponsorship/escort are denied unescorted access to FLW and are directed not to return to FLW without DOD sponsorship/escort. Future attempts to access FLW without DOD sponsorship/escort may result in criminal prosecution.

f. Any action, assistance, or support to provide or attempt to provide access to a disqualified or previously disqualified person may result in administrative and/or criminal prosecution.

Chapter 6
PHYSICAL SECURITY EQUIPMENT

6-1. Procurement

a. Proposed purchases of PSE (e.g. IDS), Closed circuit Television, or Video Surveillance Cameras) will be coordinated through the IPSO.

b. Proposed PSE that will connect in any way to the global information grid (GIG) will be coordinated through the Network Enterprise Center (NEC) to ensure compliance with applicable DOD/DA policies and certifications.

6-2. Intrusion Detection System

a. Users with active IDS in their facilities or areas will conduct monthly user level testing and record the status of these tests on DA Form 4930. See FLW Reg 190-11, Appendix B for policy and procedures on the accountability, operation, testing and maintenance of the FLW IDS system.

b. Facilities with active IDS will maintain twelve (12) months of IDS testing history on file at the facility.

c. Requests to purchase, issue, lease, or lease renewal for commercial IDS on FLW or in the AOR will be coordinated through the IPSO and IAW AR 190-13.

Chapter 7
CRIME PREVENTION

a. Commanders/directors are responsible for establishing crime prevention awareness policy to deter criminal activity that may be directed against Government and personal property within their areas of responsibilities.

b. The Standard Form SF 701 (Activity Security Checklist) will be used to record end-of-day security checks conducted for all facilities. Completed forms will be maintained on file for 1 year.

c. The Standard Form SF 702 (Security Container Check Sheet) will be used to record opening and closing of security containers/vaults. All required information on the form will be completed. This form may also be used to record after hours security checks of facilities by guard/security force and/or unit personnel. Completed forms will be maintained on file for 1 year.

Appendix A
REFERENCES

Required Publications

AR 12-15
Joint Security Cooperation Education and Training

AR 190-5
Motor Vehicle Traffic Supervision

AR 190-11
Physical Security of Arms, Ammunition, and Explosives

AR 190–13
The Army Physical Security Program

AR 190–51
Security of Unclassified Army Property (Sensitive and Non-sensitive)

AR 380-10
Foreign Disclosure and Contacts with Foreign Representative

FLW Reg 190-11
Physical Security of Arms, Ammunition and Explosives (AA&E)

REFERENCED FORMS

Forms that have been designated “approved for electronic generation (EG)” must replicate exactly the content (wording), format (layout), and sequence (arrangement) of the official printed form. The form number of the electronically generated form and the date will be the same as the date of the current edition of the printed form.

SF 701
Activity Security Checklist

SF 702
Security Container Check Sheet

DA Form 4930
Alarm Intrusion Detection Log

FLW FORM 1907
Request for Access Waiver Packet Checklist

Appendix B
SAMPLE FLW FORM 1907

WARNING: ANY MISREPRESENTATION OR OMISSION OF INFORMATION MAY RESULT IN THE DELAY OR DENIAL OF THE REQUEST

REQUEST FOR ACCESS WAIVER PACKET CHECKLIST
Proponent Directorate of Emergency Services

PRIVACY ACT STATEMENT: 1. Authority: Secretary of the Army Directive 2014-05 and FLW Regulation 190-7, Installation Access Control. 2. Principal Purpose (S): To permit personnel, who have been denied access to FLW in accordance with the Secretary of the Army's Directive 2014-05, to apply for a denial waiver through the access waiver authority. 3. Routine Uses: Attached criminal history and other personal identifying data is used to positively identify the waiver applicant and determine an acceptable level of risk. 4. Voluntary Disclosure: ANY MISREPRESENTATION OR OMISSION OF INFORMATION MAY RESULT IN THE DELAY OR DENIAL OF THE REQUEST

Please type or print neatly; Attach additional sheets if necessary.

1. Name (*First/Middle/Last*)

2. Current Mailing Address (*Number and Street, City, State, and ZIP Code*)

3. Email address:

3a. Do you want your decision emailed back to you rather than mailed to you? Yes ☐ No ☐

4. Current Telephone Number

4a. Home: 4b. Work:

5. Reason for requesting access to FLW?

6. What job will you or are you performing on FLW?

7. Briefly explain the impact your denied access to FLW has on FLW's mission.

8. Attach your personal waiver request letter (Provide a letter in your own words, to the denial waiver authority that addresses all offenses listed in the criminal history and the circumstances related to the offense(s), along with an explanation of why the conduct should not result in a denial of access and the impact on you and the mission of FLW as a result of this denial).	Letter is attached	Yes ☐ No ☐
9. Attach a copy of your certified criminal history including all convictions and arrests from all States with your records.	Criminal history attached	Yes ☐ No ☐
10. Attach a copy of Government Sponsor/Point of Contact memorandum of waiver support or non-support.	Government POC memo attached	Yes ☐ No ☐
11. If applicable obtain a letter of recommendation from employer that addresses performance and support of waiver.	Letter is attached	Yes ☐ No ☐

12. Have you been denied access by any other federal organization? Yes ☐ No ☐

12a. If yes, indicate the reason for the denial.

FLW FORM 1907, JUN 2015

Glossary
Section I - Acronyms

AA&E
Arms, Ammunition, and Explosives

AAFES
Army and Air Force Exchange Service

AOR
Area of Responsibility

AR
Army Regulation

C4IM
Command, Control, Communications, Computers, and Information Management

CAC
Command Access Card

DA
Department of the Army

DECA
Defense Commissary Agency

DES
Directorate of Emergency Services

DFMWR
Directorate of Family Morale, Welfare, and Recreation

DHS
Department of Homeland Security

DOD
Department of Defense

DPTMS
Directorate of Plans, Training, Mobilization, and Security

FLW
Fort Leonard Wood

FPCON
Force Protection Condition

GIG
Global Information Grid

GLWACH
General Leonard Wood Army Community Hospital

IACPS
Installation Access Control Points

IAW
In Accordance With

IDS
Intrusion Detection System

IHG
InterContinental Hotel Group

IPSO
Installation Physical Security Officer

LRC
Logistic Readiness Center

MEVA
Mission Essential or Vulnerable Area

MWR
Morale, Welfare, and Recreation

NAF
Non-appropriated Funds

NEC
Network Enterprise Center

NCIC
National Crime Information Center

NTE
Not to Exceed

POC
Point of contact

POV
Privately Owned Vehicle

PS
Physical Security

PSE
Physical Security Equipment

PSI
Physical Security Inspector/Inspection

PSO
Physical Security Officer

PX
Post Exchange

RAM
Random Antiterrorism Measure

SOP
Standard Operating Procedure

TWIC
Transportation Worker Identification Credential

VHIC
Veterans Health Identification Card

VIC
Veterans Identification Card

TERMS
Section II

Installation Interior Guard: A commitment assigned to major subordinate commanders to provide guards to designated facilities.

Internal Security: The security resulting from the establishment of an interior guard to affect the safety and security of property.

Unit guard: An interior guard of a command established to increase internal security of its units, activities, and facilities.

Access control: Permitting or denying the use of a particular resource by a particular entity.

Installation access control point: Points along an installation (site) boundary that represent an initial security screening point for vehicles and pedestrians entering the installation.

Ammunition: See AR 190-11.

Antiterrorism: See AR 525-13.

Arms: See AR 190-11.

Army Command: See AR 10-87.

Asset: Any Government/DOD/Army resource requiring protection.

Charrette: A collaborative session in which a group of designers drafts a solution to a design problem.

Closed post: A site or activity to which ground and water access is controlled at all times by perimeter barriers with limited, manned entry control points.

Controlled area: See restricted area.

Crime prevention: The anticipation, recognition, and appraisal of a crime risk, and initiation of some action to remove or reduce it. Crime prevention is a direct crime control method that applies to before-the-fact efforts to reduce criminal opportunity, protect potential human victims, and prevent property loss.

Defense critical asset: An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DOD to fulfill its missions.

Entry control: In terms of this regulation, security actions, procedures, equipment, and techniques, employed within restricted areas to ensure that persons who are present in the areas at any time have authority and official reason for being present.

Exception: An approved permanent continuation of a deviation from this regulation in which the requirements are not being met and the approving authority determines it is inappropriate to meet the requirements. Compensatory security measures are required to provide adequate security for the deviation.

Exclusion area: See restricted area.

Explosives: See AR 190-11.

Facility: Any single building, project, or site.

Force Protection Conditions: See AR 525-13.

Global Information Grid: See DODD 8100.1.

Installations: A grouping of facilities located in the same vicinity that support particular functions.

Intrusion detection system: Electronic components including sensors, control units, transmission lines, and monitoring units that are integrated to detect one or more types of intrusion into the area protected by the system and reporting to a central monitoring station.

Limited area: See restricted area.

Lock: A mechanical or electro-mechanical fastening device intended to control access. Locks should only be considered as a device to delay intruders, not a positive bar (or a means to fully stop) unauthorized entry since any lock can eventually be defeated by expert manipulation or by force. For high security padlocks, refer to MIL-P-43607. For high security padlocks with a shrouded shackle, refer to NSN 5340-01-217-5068. For high security padlocks with a horizontal sliding bolt, refer to NSN 5340-00-799-8248. For high security shrouded hasps to be used with high security padlocks, refer to MIL SPEC MIL-H-43905 or MIL-H-29181A. For low security padlocks with a hardened steel shackle and body, use Commercial Item Description A-A-1927. For low security padlocks with a chain, use NSN 5340-00-158-3807. For low security padlocks without a chain, use NSN 5340-00-158-3805. For hasps and staples for low security padlocks that are of heavy pattern steel, securely fastened them to the structure with smooth-headed bolts, rivets, or welding to prevent removal. For GSA approved changeable three-position padlocks, use FED SPEC FF-P-110. Refer questions to the DOD Lock Program Technical Manager, Naval Facilities Engineering Service Center, Code C66, 560 Center Drive, Port Hueneme, CA 93043-4328 (DSN 551-1567 or -1212).

Mission essential vulnerable areas: A facility or area that is essential to the mission because of the assets or capabilities located within and (or) is vulnerable to threat groups, tactics and weapons.

MEVAs can be areas that house information, equipment, property or personnel. They are recommended for MEVA status by the Provost Marshal and approved by the Commander. The term MEVA is not mutually inclusive (mission essential *and* vulnerable). It may be mission essential, but not particularly vulnerable to a known threat. In contrast, it may be vulnerable to a threat, but not particularly essential to the mission. Understanding the difference is crucial for well-informed prioritization of resources.

Physical security: A combination of physical protective measures and security procedural measures employed to safeguard personnel, property, operations, equipment, facilities, materiel, and information against loss, misuse, theft, damage or destruction by disaffected persons, vandals, activists, extremist protesters, criminals, terrorists, saboteurs and spies.

Physical security equipment: An overarching term for items, devices and systems used primarily to protect resources to include nuclear, chemical, and other munitions, personnel, and installations, and to safeguard national security information and material, including the destruction of such information and material both by routine means and by emergency destruct measures.
Physical Security Inspection: A formal, recorded assessment of physical procedures and measures implemented by a unit or activity to protect its assets.

Physical security measures: Measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. In contrast with security procedural measures that often involve personnel; these measures are usually permanent and involve expenditure of funds. Examples of physical protective measures are barriers, intrusion detection systems, locks and keys.

Physical Security Plan: A comprehensive written plan providing proper and economical use of personnel, land, and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

Physical security procedures: See physical security.

Physical Security Program: The interrelationship of various components that complement each other to produce a comprehensive approach to security matters. These components include, as a minimum, the Physical Security Plan, Physical Security Inspections and Surveys, participation in committees and fusion cells, and a continuing assessment of the physical security posture.

Physical security resource plan: A plan developed by the physical security officer, and approved by the responsible commander that identifies physical security needs and shows proposed, prioritized procurement of those needs.

Physical security survey: A formal, recorded assessment of the installation Physical Security Program.

Protection in depth: A system providing several supplementary security barriers. For example, a perimeter fence, a secure building, a vault, and a locked container provide four layers of protection. (DOD 5100.76–M)

Restricted area: An enclosed area with an established boundary that prevents admission unless special conditions or controls are met that safeguard, personnel, property or material within. These areas are not to be confused with those designated FAA areas over which aircraft flight is restricted. All restricted areas must be marked and have the ability to control access to the designated 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. The three classes of restricted areas are controlled, limited and exclusion.

Controlled area: A controlled area is a designated restricted area that denies access to the general public unless certain entry controls are met. This type of area has the least restrictive conditions and usually the controls required for entry include a military identification card or proof of identification by some other federal or state government document, and a need for access. Once authorized entry, movement within the area is not controlled. An example of a controlled area is an Army installation or facility where entry onto the installation or facility is permitted at the Access Control Point (ACP). A controlled area may also be a building or business that is not accessible by the general public because entry is controlled by proof of identification that the individual is an active or retired member of the military (e.g., commissary, Post Exchange).

Limited area: A limited area is a designated restricted area that is more restrictive than a controlled area because in addition to the need for access and proof of positive identification, entry is limited to only those individuals whose names have been previously placed on an entry control roster (ECR) signed by the controlling authority (installation/activity commander) or who have been enrolled in an Electronic Access Control System (EACS), or are part of an approved exchange badge system. Entry is granted to those limited individuals listed on the ECR, enrolled in the EACS, or members of an exchange badge system after verification at the Entry Control Facility (ECF). Movement within a limited area is not controlled for those authorized unescorted entry. A limited area is normally a buffer zone for an exclusion zone because access to the security interest contained within the exclusion area remains prohibited. Commanders may require escorts for uncleared personnel with a need for entry into the limited area.

Exclusion area: An exclusion area is a designated restricted area that contains a security interest or other material of such vital importance that proximity resulting from entry into the area constitutes access to such security interest or material. Therefore entry into an exclusion area is more restrictive than into a limited area. An exclusion area is normally located within a limited area. In addition to those conditions required for entry into a limited area, entry is excluded from everyone unless they are identified through an ECR, EACS, or exchange badge system for the exclusion area and can meet two conditions: (1) The person must be a current member of the Personnel Reliability Program (PRP), and (2) the person is a participant in a two-person access requirement within the area. Movement within an exclusion area is controlled by the two-person rule. All other individuals allowed entry into an exclusion area must be escorted by person who can satisfy the previous two conditions. Persons under escort cannot satisfy the two-person requirement and are not considered to have access to the security interest.

Risk: The degree or likelihood of loss of an asset. Factors that determine risk are the value of the asset to its user in terms of mission criticality, replace ability, and relative value and the likelihood of aggressor activity in terms of the attractiveness of the asset to the aggressor, the history of or potential for aggressor activity, and the vulnerability of the asset.

Risk analysis: Method of examining various risk factors to determine the risk value of likelihood of resource loss. This analysis will be used to decide the level of security warranted for protection of resources.

Risk factors: Elements that make up the total degree of resource loss liability. Factors to be considered in a risk analysis include the importance of the resource to mission accomplishment; the cost, volume, criticality and vulnerabilities of the resources; and the severity of threats to the resources.

Security identification card: An official distinctive identification (pass or card) that identifies and authorizes the possessor to be physically present in a designated restricted area.

Security engineering: The application of engineering principles to the protection of assets against various threats through the application of construction and equipment application.

Security procedural measures: Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Task critical asset: An asset of such extraordinary importance to DOD operations that its unavailability would have a very serious, debilitating effect on the ability of the Army to execute the task or mission essential task it supports.

Tenant activity: A unit or activity of one Government agency, military department, or command that occupies facilities on an installation of another military department or command and that receives supplies or other support services from that installation.

Terrorism: The calculated use of violence or the threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals, that are generally political, religious, or ideological.

Waiver: Temporary relief from specific standards imposed by regulation, pending actions accomplishment of actions that will conform to the standards required. Compensatory measures are required.