


21 July 2015

Military Police
INSTALLATION ACCESS CONTROL

FOR THE COMMANDER:

OFFICIAL:

DAVID G. RAY
COL, GS
Acting Chief of Staff



JESSE FRENCH
Director, Human Resources

History. This publication is a new regulation.

Summary. This regulation establishes the philosophy, policy, format, guidance, and standardized procedures for the planning, coordination, and execution of the Installation Access Control Program.

Applicability. This regulation is applicable to all persons, vehicles, and equipment that access or attempt to access the boundaries and/or facilities of the Fort Leonard Wood (FLW) military installation.

Proponent and execution authority. The proponent agency of this regulation is the Provost Marshal.

Supplementation. Supplementation of this regulation is prohibited without prior approval by Headquarters, U.S. Army Maneuver Support Center of Excellence (MSCoE).

Administrative Note: The words "he" and "his" used herein are intended to include both the masculine and feminine genders, except where otherwise noted.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, MSCoE (IMNE-LNW-ES), Fort Leonard Wood, MO 65473-5000.

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

Table of Contents

Page

Paragraph 1. Purpose	1
Paragraph 2. References and forms	1
Paragraph 3. Explanation of acronyms, abbreviations, and special terms	1
Paragraph 4. General	1
Paragraph 5. Responsibilities	1
Paragraph 6. Policy	3
Paragraph 7. Valid unescorted and non-valid escorted access determinations	6
Paragraph 8. FLW-recognized DOD access identity documents	8
Paragraph 9. FLW-recognized non-DOD access identity documents	9
Paragraph 10. Sponsoring authority	10
Paragraph 11. Organizational sponsoring authorities	11
Paragraph 12. Vehicle access	11
Paragraph 13. FLW access card and visitor pass	12
Paragraph 14. Mission Essential Tier System (METS)	12
Paragraph 15. Special event access control	13
Paragraph 16. Special event installation access control points (IACPs)	15
Paragraph 17. Special event privately owned vehicle (POV) access	15
Paragraph 18. Trusted traveler program	15
Paragraph 19. (Punitive) FLW access policy violations	15
Appendix A. References and forms.....	16
Appendix B. Sample of FLW Form 1907	20
Appendix C. Example of a special events staffing paper.....	21
Appendix D. Example of a DD Form 577	22
Glossary	23

1. Purpose

This regulation provides policy and procedures for controlling access to the FLW Army installation as directed by the senior commander.

- a. Assists security personnel in providing a continuous and appropriate level of security for FLW access control and facilitates rapid transitions to higher levels of force protection conditions (FPCON).
- b. Provides standards and procedures for accessing FLW by authorized personnel, vehicles, and material and denying access to unauthorized personnel, vehicles, and materials. A function of this is to verify the identity of individuals entering FLW and identify those with known or possible criminal or terroristic intentions that may pose a threat to good order and discipline or to health and safety on the installation.
- c. Provides minimum requirements for use in the contracting process to authenticate the claimed identity of an individual or to identify individuals attempting to misrepresent themselves and gain unauthorized access to FLW.
- d. Addresses minimum requirements for personnel requesting entry to FLW through established installation access control points (IACPs), the co-located airport, and internal facilities with a validated need to access (such as maintenance, landscaping, and construction) on a recurring basis, as well as those personnel conducting business or visiting with FLW organizations on a nonrecurring or noncontract basis (such as taxi drivers, food delivery, Friends of FLW, those using FLW as a thoroughfare, or those using the co-located airport).
- e. Complements other Department of Defense (DOD) or Department of the Army (DA) publications and does not eliminate their requirements for developing and maintaining a practical, economical, and effective access control program.

2. References and forms

All required and related publications, prescribed, and referenced forms within this regulation are listed in appendix A.

3. Explanation of acronyms, abbreviations, and special terms

Abbreviations and special terms used in this regulation are explained in the glossary at the end of this publication.

4. General

The FLW Army Installation, defined by man-made and natural boundaries to include the co-located airport, is designated as a restricted area IAW AR 190-13 to which access is controlled. Access control is an integral part of the Installation's Physical Security Program as it regulates, for security purposes, the flow of personnel, vehicles, and materials entering and exiting FLW. It subjects all personnel and their vehicles to safety and security inspections prior to gaining access to FLW and prohibits unauthorized photographing or drawings of restricted areas. Inconvenience to organizations or individuals will not be a reason to circumvent or modify access control security procedures established by this regulation.

5. Responsibilities

- a. The Garrison Commander will—

(1) Ensure, at a minimum, access control is conducted at all operational 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.

(2) 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.

(3) Allocate the necessary resources to enforce established installation access control measures.

(4) Maintain a visitor control program for non-DOD affiliated individuals requesting access to enter FLW.

(5) Enforce the removal of, or deny access to, persons who threaten the order, security, discipline or health and safety on the installation.

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

b. Commanders and directors will—

(1) Establish, in writing, access control procedures for restricted areas as part of physical security plans/standing operating procedures (SOPs) within their scope of responsibility in accordance with (IAW) AR 190-13 and this regulation.

(2) Appoint in writing on DD Form 577 (Appointment/Termination Record – Authorized Signature) unit/organization sponsoring authorities/points of contact (POCs) responsible for validating access requests for contractors, vendors, service providers or visitors pertaining to their organizational requirements or events.

(3) 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.

(4) Establish at the direction of the senior commander unit/activity procedures to ensure all personnel register vehicles IAW AR 190-5 and this regulation.

c. Commanders of military units will provide support as tasked for increased levels of installation access control IAW the current FLW Emergency Guard Force Plan.

d. DOD affiliated and non-DOD affiliated personnel will—

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

(2) 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.

e. Director, Emergency Services will—

(1) Implement access control procedures and SOP for all IACPs based on the current FPCON IAW applicable directives and this regulation.

(2) Be the proponent for installation access control.

(3) Control security forces and operations at all FLW IACPs.

(4) 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.

(5) Manage and implement FLW visitor and vehicle registration procedures.

(6) Ensure that the Visitor Control Center (VCC) and access control personnel adhere to the requirements of this regulation and that authorized personnel are issued FLW passes (when authorized and applicable).

(7) Ensure, in coordination with unit commanders on the installation, that when a family care plan is executed, the care giver is properly vetted IAW this regulation prior to allowing access on to the installation.

f. Director, Logistics Readiness Center (LRC) will provide maintenance service and support for intrusion detection systems (IDS) located at IACPs.

g. Director, Network Enterprise Center (NEC) will provide for all required communication/data lines dedicated solely for IDS and communication functions at IACPs in accordance with command, control, communications, computers, and information management (C4IM) service catalog and service level agreement policy.

h. Public Affairs Office (PAO) will—

(1) Be the single point of contact for sponsorship of public or private non-DOD affiliated media personnel.

(2) 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.

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

i. Directorate of Plans, Training, Mobilization, and Security (DPTMS) will—

(1) Review all special event staffing papers.

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

6. Policy

The Directorate of Emergency Services (DES) is the authority for granting or denying access to FLW. The DES Director (Provost Marshal); Deputy Director; Operations Officer; 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 7), a DOD-affiliated sponsorship, current state vehicle registration, proof of current

vehicle insurance, current state-issued driver's license, and assessment of an authorized FLW identification (ID) document.

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 (this includes valid, current FLW passes) 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 15 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 (SCIC), available United States Government (USG) information databases, and/or the access control system denied access list, driving suspension list, and the FLW debarment list.

g. All non-DOD affiliated personnel requiring access to FLW will be sponsored by an authorized DOD-credentialed individual or DOD organization, possessing sponsorship authority as specified in paragraph 10. 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. DOD organizations and activities needing to establish recurring access authorization for non-DOD personnel that do not meet common access card (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 will submit their request for an installation pass to their sponsor using the FLW secure preregistration pass 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 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 to FLW will be determined by an analysis of information obtained through authoritative government data sources. At a minimum, FLW will query the NCIC III and the Terrorist Screening Database (TSDB) 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 installation is unable to verify the individual's claimed identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.

(3) The individual has 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, 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.

j. Persons attempting further access to FLW after being denied access based on the criteria listed above that have not received an approved access waiver may be subject to criminal prosecution.

k. In the event that an individual is denied 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 will be responsible for submitting the waiver request to the senior commander or designated representative.

(2) Obtain a certified copy of their complete criminal history, to include all arrests and convictions.

(3) Obtain 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, the sponsor must inform the senior commander or the designated representative so the unescorted access to the installation is no longer authorized.

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

(a) Nature and seriousness of the conduct.

(b) Specific circumstances surrounding the conduct.

(5) Obtain a letter of reference or recommendation from employer if applicable.

7. Valid unescorted and non-valid escorted access determinations

Persons requesting to enter FLW must have a valid need 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 need 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, service providers to the installation (such as food delivery, taxi driver, or tow truck drivers).

(b) Visiting the Army museums or special events.

(c) Using morale, welfare, and recreation (MWR) facilities.

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

(e) Hunting and fishing on FLW.

(2) 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 15 of this regulation based on the current FPCON and risk assessment.

(3) Individuals affiliated with the DA Survivors Outreach Services (SOS) Program are authorized unescorted access to FLW IAW paragraph 6i above. The date the NCIC III check is conducted must be typed on the DA Form 1602 (Civilian Identification) when issued.

(4) Official foreign visitors such as foreign liaison officers, foreign exchange personnel, and cooperative program personnel subject to the provisions of AR 380-10 will be granted unescorted visitor status. The foreign visit system confirmation module will be used to confirm the proposed official

visit to FLW. A check of NCIC III and TSDB records will not be conducted for these official foreign visitors. For additional information or guidance contact the FLW Foreign Disclosure Officer.

(5) When emergency response vehicles/personnel enter FLW 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.

(6) Non-DOD affiliated clergy sponsored by the Installation Chaplain's Services that do not meet CAC eligibility requirements may receive an unescorted pass for "official business only."

(7) Non-DOD affiliated 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.

(8) Directorate of Family and Morale, Welfare, and Recreation (DFMWR)/nonappropriate fund (NAF) flex employees that do not meet CAC eligibility requirements may receive an unescorted pass for "official business only."

(9) Moving and freight companies approved and sponsored to operate on FLW by LRC Transportation Division that do not meet CAC eligibility requirements may receive unescorted access passes for "official business only" for a period NTE 180 days.

(10) School faculty and parents of nonmilitary affiliated children attending a Waynesville R-6 School District 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.

(11) Veterans Administration medical 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.

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

(1) Patronage of eating establishments on FLW (such as Burger King, Taco Johns, or Post Exchange [PX] Food Court), shopping at the Army and Air Force Exchange Service (AAFES) retail establishments, or general sightseeing on FLW 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 and do not have a valid need for access but may have a one-time or intermittent request to access FLW. Visitors require a DOD sponsor, will be signed-in at the gate of entry, must be issued a FLW pass, and must be escorted by a DOD ID cardholder at all times while on FLW.

(3) 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. Foreign nationals without DOD sponsorship/escort will be denied access to FLW will be directed not to return to FLW without DOD sponsorship/escort and will be informed that future attempts to access FLW without DOD sponsorship/escort may result in criminal prosecution.

(4) 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.

8. FLW-recognized DOD access identity documents

a. The following DOD-identity documents are recognized for unescorted access to FLW without needing NCIC III vetting once the document and individual holder are verified.

(1) Common Access Card (CAC), DoD CIO/OUUSD (P&R). The CAC is the principal access control token and standard ID card for Active duty, National Guard, and Reserve military personnel, DOD civilian employees, eligible contractors, and some designated foreign nationals.

(2) CAC (chipless) (DOD Civilian Retiree Identification Card). Effective 26 Aug 2009 DOD civilian retirees may be issued a chipless CAC.

(3) DD Form 2(ACT) (Armed Forces of the United States Geneva Convention Identification Card).

(4) DD Form 2(RES) (Armed Forces of the United States Geneva Conventions Identification Card).

(5) DD Form 2(RET) (United States Uniformed Identification Card [Retired]).

(6) DD Form 2A(RES) (Armed Forces of the United States Identification Card [Reserve]).

(7) DD Form 2S (ACT) Green (Armed Forces of the United States Geneva Convention Identification Card).

(8) DD Form 2S (RES RET) Red (Armed Forces of the United States Identification Card [Reserve] [Retired]).

(9) DD Form 1173 (Uniformed Services Identification and Privilege Card).

b. The following DOD-identity documents are recognized for unescorted access to FLW after favorable NCIC III vetting once the document and individual holder are verified.

(1) DD Form 2764 (United States DOD/Uniformed Services Civilian Geneva Convention Identification Card).

(2) AF Form 354 (Air Force Civilian Identification Card).

(3) DD Form 489 (Geneva Conventions Identity Card for Persons Who Accompany the Armed Forces).

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

(5) DA Form 1602 (Civilian Identification).

(6) DD Form 1934 (Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces).

(7) FLW locally produced installation access card or pass.

(8) FLW Form 1817 (Maneuver Support Center of Excellence Temporary Vehicle Pass), temporary 24-72 hour visitor pass when accompanied by a valid state-issued driver's license for the individual to whom the pass was issued.

9. 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 a FLW access card or visitor pass for unescorted or escorted access as directed by the senior commander or designated representative. 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 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) employee ID cards: PS Form 5140 (Non-Postal Service Contract Employee) and PS Form 4098 (Employee Identification Card) (NCIC III vetting not required).

(5) All forms of U.S. Department of Homeland Security (DHS) ID Cards (NCIC III vetting not required).

(6) U.S. Government Investigative Services ID Card (NCIC III vetting not required).

(7) Transportation Security Agency (TSA), Transportation Worker Identification Credential (TWIC).

(8) U.S. Government-issued authenticated Federal personal identification verification (PIV) credentials (NCIC III vetting not required).

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.

10. Sponsoring authority

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. DOD sponsors must be affiliated with FLW to exercise sponsoring authority.

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 individuals 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 secure preregistration pass portal. DOD POC/sponsors may contact the VCC for information on how visitors may access the preregistration pass portal.

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

(3) When the preregistration pass portal is not functioning, DOD sponsors will send request memorandums via e-mail with digital CAC signature to the VCC <*usarmy.leonardwood.usag.mbx.desvisctr@mail.mil*> or drop off in person and show a valid DOD ID card to verify sponsorship authority. Memorandum 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 authority on FLW.

e. NAF, AAFES, Defense Commissary Agency (DeCA) employees when designated by their organization on DD Form 577 as a DOD-sponsoring authority and in possession of a valid DOD ID card may sponsor 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 on a recurring basis, the Installation Physical Security Officer will be the validating official and sponsoring authority.

11. Organizational sponsoring authorities

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

a. All DOD-sponsoring activities/organizations will use DD Form 577 to designate individual(s) approved to authenticate and coordinate requests for access for that organization with the VCC. The VCC will maintain this form on file and verify current status of sponsoring authorities with the organization at a minimum semi-annually. DD Forms 577 will be resubmitted annually or upon change of appointment authority within the organization.

b. Only DOD-sponsoring authorities on DD Forms 577 will be authorized to authenticate entry authorization lists (EALs) and forward these to the VCC for processing.

c. All sponsors must be a DOD ID cardholder.

d. Walk-in customers and preregistration pass 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. When applicable, VCC personnel will contact sponsoring authorities to schedule when applicants may pick up their FLW pass.

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 the 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.

12. Vehicle access

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

a. Access may be denied to vehicles that are obviously defective. 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.

b. 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.

13. FLW access card and visitor pass

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

a. FLW 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.

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

c. All FLW cards and passes will be subject to current FPCON and day/time restrictions. Sponsoring authorities will set individual FPCON restrictions based on the METS (paragraph 14 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 a FLW 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. 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.

14. 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 FLW 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 vetting. The AT Office will verify lists and submit to the Installation Operations Center (IOC)/Emergency Operations Center (EOC) and DES Security Operations Branch 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 a FLW 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 is 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 (DFAC) 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).

15. 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 on FLW 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.

a. DOD organizations sponsoring or responsible for special events on FLW must submit a FLW Form 1416 (MSCoE Staffing Paper) (example provided in appendix C) 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.

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.

e. FLW visitor passes may be processed via the preregistration pass portal or e-mailed to the VCC at <usarmy.leonardwood.usag.mbx.desvisctr@mail.mil>. Visitors must include the information required by the preregistration pass portal when requesting a FLW 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 within the VCC, building 100, where it will be processed for NCIC III and U.S. Immigration and Customs Enforcement (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 Branch to obtain guidance on submitting applications for visitors unable to access the preregistration pass portal or follow paragraph 15e.

i. U.S. citizens attending student family days and graduations may be authorized temporary unescorted access to FLW on the dates of those events without a FLW pass. For these personnel attending special events and activities, NCIC III screening may be waived. Person(s) requesting access must possess a valid, current 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 access to FLW during the hours of 2100 – 0500 will require DoD ID cardholder sponsorship and a FLW Form 1817.

16. Special event installation access control points (IACPs)

DES may designate specific gate(s) for the processing of special event person(s)/vehicle(s) where security measures will be conducted prior to allowing entrance onto the installation. Gate(s) will be staffed with appropriate security personnel and resources for a time frame to adequately accommodate a reasonable yet secure flow of traffic onto FLW.

17. Special event privately owned vehicle (POV) access

Visitors requesting unescorted access to FLW 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.

18. Trusted traveler program

This program may be initiated as directed by the senior commander based on the current FPCON and IAW current DOD/DA policies and procedures.

19. (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.

Appendix A

REFERENCES AND FORMS

Section I. Required Publications

AR 190-5

Motor Vehicle Traffic Supervision (Cited in para 12.)

AR 190-11

Physical Security of Arms, Ammunition, and Explosives (Cited in Glossary, Section II. Terms.)

AR 190-13

The Army Physical Security Program (Cited in paras 4, 5b(1), 7a(2), and 12b.)

AR 380-10

Foreign Disclosure and Contacts with Foreign Representatives (Cited in paras 7a(4) and 7b(3).)

AR 525-13

Antiterrorism (Cited in Glossary, Section II. Terms.)

FLW Emergency Guard Force Plan (Cited in para 5c.)

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (Cited in Glossary, Section II. Terms.)

Section II. Related Publications

DOD 5200.08-R

Physical Security Program

DODI 2000.16

DOD Antiterrorism (AT) Standards

AR 190-16

Physical Security

AR 190-51

Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 190-56

The Army Civilian Police and Security Guard Program

AR 600-8-14

Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel

FLW Reg 190-5

Motor Vehicle Traffic Supervision on Fort Leonard Wood

FLW Reg 190-6

Registration and Control of Privately Owned Firearms and Other Weapons on Fort Leonard Wood

FLW Reg 190-11

Physical Security of Arms, Ammunition, and Explosives

ATP 3-39.32
Physical Security

DTM 09-012
Interim Policy Guidance for DOD Physical Access Control

Secretary of the Army Directive 2014-05
Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors

HQDA EXORD 033-15
Installation Access Control and Reporting

HQ IMCOM OPORD 15-031
Implement Access Control Procedures at IMCOM Installations

HQ TRADOC OPORD 14-021
Implementing Guidance for HQDA EXORD 033-15

USNORTHCOM OPORD 05-01B
Physical Security - Personnel Identity Validation for Access

US Army Installation Management Command Force Protection OPORD #09-001
Installation Access Control Program

Title 32
National Defense, Subpart C – Motor Vehicle Registration

UFC 4-22-01, Security Engineering: Entry Control Facilities/Access Control Points (Cited in Glossary, Section II. Terms.)

HQDA Message DTG: 152028Z May 07
Installation Force Protection Message

HQDA Message DTG: 101616Z Oct 03
Department of the Army Installation Access Control Program

Section III. Prescribed Forms

FLW Form 1817
Maneuver Support Center of Excellence Temporary Vehicle Pass (Prescribed in paras 8b(8), 13f, and 15i.)

FLW Form 1907
Request for Access Waiver Packet Checklist (Prescribed in 6k(1).)

Section IV. 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 will be shown as –R–E and the date will be the same as the date of the current edition of the printed form.

AF Form 354
Air Force Civilian Identification Card

DA Form 1602
Department of the Army Civilian Identification Card.

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2(ACT)
Armed Forces of the United States Geneva Convention Identification Card. This is an inactive form.

DD Form 2(RES)
Armed Forces of the United States Geneva Conventions Identification Card. This is an inactive form.

DD Form 2(RET)
United States Uniformed Identification Card (Retired). This is an inactive form.

DD Form 2A(RES)
Armed Forces of the United States Identification Card (Reserve)

DD Form 2S (ACT) Green
Armed Forces of the United States Geneva Convention Identification Card. This is an inactive form.

DD Form 2S (RES RET) Red
Armed Forces of the United States Identification Card (Reserve) (Retired)

DD Form 489
Geneva Conventions Identity Card for Persons Who Accompany the Armed Forces. This is an inactive form.

DD Form 577
Appointment/Termination Record – Authorized Signature

DD Form 1173
Uniformed Services Identification and Privilege Card

DD Form 2764
United States DOD/Uniformed Services Civilian Geneva Convention Identification Card

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

DD Form 1934
Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces.

FLW Form 1416
MSCoE Staffing Paper

Form I-94
Arrival-Departure Record

Form I-151
Permanent Resident Card

Form I-327
Reentry Permit

Form I-551
Alien Registration Receipt Card

Form I-571
Refugee Travel Document

Form I-688
Temporary Resident Card

Form I-688A
Employment Authorization Card

Form I-688B
Employment Authorization Document

PS Form 4098
Employee Identification Card

PS Form 5140
Non-Postal Service Contract Employee

Appendix B
SAMPLE OF A 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 (<i>First/Middle/Last</i>)		
2. Current Mailing Address (<i>Number and Street, City, State, and ZIP Code</i>)		
3. Email address:		
3a. Do you want your decision emailed back to you rather than mailed to you? Yes <input type="checkbox"/> No <input type="checkbox"/>		
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 <input type="checkbox"/> No <input type="checkbox"/>
9. Attach a copy of your certified criminal history including all convictions and arrests from all States with your records.	Criminal history attached	Yes <input type="checkbox"/> No <input type="checkbox"/>
10. Attach a copy of Government Sponsor/Point of Contact memorandum of waiver support or non-support.	Government POC memo attached	Yes <input type="checkbox"/> No <input type="checkbox"/>
11. If applicable obtain a letter of recommendation from employer that addresses performance and support of waiver.	Letter is attached	Yes <input type="checkbox"/> No <input type="checkbox"/>
12. Have you been denied access by any other federal organization? Yes <input type="checkbox"/> No <input type="checkbox"/>		
12a. If yes, indicate the reason for the denial.		

FLW FORM 1907, JUN 2015

Figure B-1. Sample of A FLW Form 1907

Appendix C
EXAMPLE OF A SPECIAL EVENTS STAFFING PAPER

MSCoE STAFFING PAPER						SGS Control Number	
ACTION OFFICER				COMMAND GROUP ACTION			
NAME				ORDER	NOTED	CONCUR	APPROVAL
ACTIVITY				CG			
DATE	PHONE	OFFICE SYMBOL		DCG			
TASK NUMBER	SUSPENSE			CS			
INFORMATION	<input checked="" type="checkbox"/>	APPROVAL AND SIGNATURE		CSM			
APPROVAL	APPROVAL AND INITIALS			SGS			
SUBJECT:							
Access Control Waiver Request for (provide EVENT NAME and DATE(s) of event)							
<p>1. PURPOSE. Obtain decision to designate (EVENT NAME) as a special event for waiving National Crime Information Center (NCIC) Interstate Identification Index (III) vetting and allow unescorted access to Fort Leonard Wood for personnel attending this event.</p> <p>2. RECOMMENDATION. The the Garrison Commander review attached risk assessment along with the below discussion comments and approve or deny by signing below.</p> <p>3. DISCUSSION. (Organization will provide justification to support request for special event status.)</p> <div style="text-align: center; margin-top: 100px;"> <p>(Insert signature block for Garrison Commander - SAMPLE BELOW)</p> <div style="display: flex; justify-content: space-around; align-items: flex-end;"> <div style="text-align: left;"> <p>_____ Approved</p> <p>_____ Disapproved</p> </div> <div style="text-align: left;"> <p>ANDREW M. HERBST COL, CM Commanding</p> </div> </div> </div>							
CHAIN OF COMMAND APPROVAL				COORDINATION			
COMMANDER/DIRECTOR	INITIALS	DATE	OFFICE-RESPONSE-DATE	(CONTINUATION)			
Antiterrorism Officer, DPTMS							

Figure C-1. Example of FLW Form 1416 for a special event

Appendix D

EXAMPLE OF A DD FORM 577

APPOINTMENT/TERMINATION RECORD - AUTHORIZED SIGNATURE <i>(Read Privacy Act Statement and Instructions before completing form.)</i>		
PRIVACY ACT STATEMENT AUTHORITY: E.O. 9397, 31 U.S.C. Sections 3325, 3528, DoDFMR, 7000.14-R, Vol. 5. PRINCIPAL PURPOSE(S): To maintain a record of appointment and termination of appointment of persons to any of the positions listed in Item 6, and to identify the duties associated with this appointment. SORN T1300 (http://dpclo.defense.gov/Privacy/SORNSIndex/DODComponentArticleView/tabid/7489/Article/6235/t1300.aspx) ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U.S.C Section 552a(b) of the Privacy Act of 1974, as amended. It may also be disclosed outside of the Department of Defense (DoD) to the the Federal Reserve Banks to verify authority of the appointed individuals to issue Treasury checks. In addition, other Federal, State and local government agencies, which have identified a need to know, may obtain this information for the purpose(s) identified in the DoD Blanket Routine Uses published at: http://dpclo.defense.gov/Privacy/SORNSIndex/BlanketRoutineUses.aspx . DISCLOSURE Voluntary; however, failure to provide the requested information may preclude appointments.		
SECTION I - APPOINTEE		
1. NAME <i>(First, Middle Initial, Last and Rank or Grade)</i> John E. Doe, GS08	2. DoD ID NUMBER EDIPI #	3. TITLE DUTY POSITION
4. DOD COMPONENT/ORGANIZATION Organization/Unit Name	5. ADDRESS <i>(Include ZIP Code, email address, and telephone number with area code and DSN)</i> Organization/Unit address .mil email address contact phone number	
6. POSITION TO WHICH APPOINTED <i>(X appropriate box - one only. Checking more than one invalidates the appointment.)</i> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <input type="checkbox"/> DISBURSING OFFICER: DSSN _____ <input type="checkbox"/> DEPUTY DISBURSING OFFICER: DSSN _____ <input checked="" type="checkbox"/> CERTIFYING OFFICER <input type="checkbox"/> DEPARTMENTAL ACCOUNTABLE OFFICIAL </div> <div style="width: 30%;"> <input type="checkbox"/> CASHIER <input type="checkbox"/> PAYING AGENT <input type="checkbox"/> COLLECTIONS AGENT <input type="checkbox"/> DISBURSING AGENT </div> <div style="width: 30%;"> <input type="checkbox"/> CHANGE FUND CUSTODIAN <input type="checkbox"/> IMPREST FUND CASHIER <input type="checkbox"/> SAFEKEEPING CUSTODIAN <input type="checkbox"/> ASSISTANT SAFEKEEPING CUSTODIAN </div> </div>		
7. YOU ARE APPOINTED TO SERVE IN THE POSITION IDENTIFIED IN ITEM 6. YOUR RESPONSIBILITIES INCLUDE: IAW FLW Reg 190-7, review, approve, and coordinate requests for pass applications by individuals who may require unescorted access to FLW for (organization name) with the Directorate of Emergency Services (DES), Visitor Control Center (VCC) building 100. IAW FLW Reg 190-7, review, approve, and coordinate submittal of denied access waiver packets for the Garrison Commander's action with the DES Security Operations Branch.		
8. REVIEW AND ADHERE TO THE FOLLOWING PUBLICATION(S) NEEDED TO ADEQUATELY PERFORM YOUR ASSIGNED DUTIES: AR 190-13, The Army Physical Security Program, Chapter 8 FLW Regulation 190-7, Installation Access Control Secretary of the Army Directive 2014-05		
SECTION II - APPOINTING AUTHORITY		
9. NAME <i>(First, Middle Initial, Last)</i>	10. DATE <i>(YYYYMMDD)</i>	11. DOD COMPONENT/ORGANIZATION
12. DATE <i>(YYYYMMDD)</i>		13. SIGNATURE
SECTION III - APPOINTEE ACKNOWLEDGEMENT		
I acknowledge and accept the position and responsibilities defined above. I understand that I am strictly liable to the United States for all public funds or payment certification, as appropriate, under my control. I have been counseled on my pecuniary liability applicable to this appointment and have been given written operating instructions. I certify that my official signature is shown in item 16 below.		
14. PRINTED NAME <i>(First, Middle Initial, Last)</i>	15. DATE <i>(YYYYMMDD) (Not earlier than date in Item 12 or 13)</i>	16. SIGNATURE a. DIGITAL b. MANUAL
SECTION IV - APPOINTMENT TERMINATION		
The appointment of the individual named above is hereby revoked.		17. DATE <i>(YYYYMMDD)</i>
18. APPOINTEE INITIALS		
19. NAME OF APPOINTING AUTHORITY	20. TITLE	21. APPOINTING AUTHORITY SIGNATURE

DD FORM 577, JUL 2014

PREVIOUS EDITION IS OBSOLETE.

Adobe Designer 9.0

Figure D-1. Example of a DD Form 577

Glossary

Section I. Acronyms, Abbreviations, and Brevity Codes.

AAFES Army and Air Force Exchange Service	C4IM command, control, communications, computers, and information management
ACP access control point	DA Department of the Army
ACT active	DD Department of Defense
AF Air Force	DeCA Defense Commissary Agency
AIE automated installation entry	DES Directorate of Emergency Services
AOR area of responsibility	DFAC dining facility
AR Army regulation	DFMWR Directorate of Family and Morale, Welfare, and Recreation
AT antiterrorism	DHS Department of Homeland Security
ATO antiterrorism officer	DOB date of birth
ATP Army techniques publication	DOD Department of Defense
CAC common access card	DoD CIO/OUIS (P&R) Department of Defense Chief Information Officer/Office of the Under Secretary of Defense for Personnel and Readiness
CAT crisis action team	DODI Department of Defense Instruction
CBRNE chemical, biological, radiological, nuclear, and high yield explosives	DPTMS Directorate of Plans, Training, Mobilization and Security
COR contracting officer representative	DTG date-time group
COTR contracting officer technical representative	DTM Directive-Type Memorandum
C2 Command and Control	

EACS
electronic access control system

EAL
entry authorization list

ECF
entry control facility

ECR
entry control roster

EOC
Emergency Operations Center

EOD
explosive ordnance disposal

EXORD
executive order

FAA
Federal Aviation Administration

FLW
Fort Leonard Wood

FPCON
force protection condition

GLWACH
General Leonard Wood Army Community
Hospital

HQDA
Headquarters, Department of the Army

IACP
installation access control point

IAW
in accordance with

ICE
United States Immigration and Customs
Enforcement

ID
identification

IDS
intrusion detection system

III
Interstate Identification Index

IMCOM
Installation Management Command

IOC
Installation Operations Center

KO
contracting officer

LRC
Logistics Readiness Center

METS
Mission Essential Tier System

MEVA
mission essential or vulnerable area

MSCoE
Maneuver Support Center of Excellence

MWR
morale, welfare, and recreation

NAF
nonappropriated fund

NCIC
National Crime Information Center

NEC
Network Enterprise Center

NTE
not to exceed

OPORD
operations order

PAO
Public Affairs Office

PIV
personal identification verification

POC
point of contact

POV
privately owned vehicle

PRP
Personnel Reliability Program

PS
Postal Service

PX
Post Exchange

RAM
random antiterrorism measures

RES
reserve

RET
retired

SCIC
State Crime Information Center

SNAIR
snow and ice removal

SOP
standing operating procedure

SOS
Survivors Outreach Services

TSA
Transportation Security Agency

TRADOC
Training and Doctrine Command

TWIC
transportation worker identification credential

TSDB
Terrorist Screening Database

UFC
unified facilities criteria

U.S.
United States

USNORTHCOM
United States Northern Command

USG
United States Government

VCC
Visitor Control Center

VIN
vehicle identification number

Section II. Terms.

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

Antiterrorism
See AR 525-13.

Army Access Control Points Standard Definitive Design
Provides standards to meet access control functions on Active Army installations and Reserve Component prime installations. <<https://www.us.army.mil/suite/page/441649>>

Army Standard for Access Control Points (ACPs)
Provides standards for Army ACPs. <<https://www.us.army.mil/suite/doc/8912967>>

Army Standard (Part I) and System Specifications (Part II) for Automated Installation Entry (AIE)
Provides standards for Army AIE. <<https://www.us.army.mil/suite/doc/9647105>>

Asset
Any resource requiring protection.

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.

Common Access Card (CAC)

An individual identification card displaying the cardholder's name, photo and organization. The CAC is the DOD implementation of Homeland Security Presidential Directive 12 that requires Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.

Contractor Verification System

A web-based system used to issue CACs to government-sponsored contract employees who need to use government computers.

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.

Explosives

See AR 190-11.

Facility

Any single building, project, or site.

Force Protection Conditions

See AR 525-13.

Installations

A grouping of facilities located in the same vicinity that supports particular functions.

Installation access control point

A point along an installation boundary that represents an initial security screening point for vehicles and pedestrians entering the installation.

Mission essential or vulnerable areas (MEVAs)

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.

National Crime Information Center

A computerized index of criminal justice information such as criminal record history information, fugitives, stolen properties, and missing persons. NCIC is operated by the Federal Bureau of Investigation. It is a continuous operation available to Federal, state, and local law enforcement and

other criminal justice agencies. An NCIC III check searches these databases: Wanted Person File, Foreign Fugitive File, Violent Gang and Terrorist Organization File, U.S. Secret Service File, Convicted Persons on Supervised Release File, Threat Against Peace Officer Alert File, Protection Order File, Missing Person File, State Criminal Investigation Division Only Wanted Person File, Concealed Handgun License File, Driver's License Record File, Convicted Sexual Offender Registry File, Deported Felon File, and the Unidentified Persons File.

National Defense Area

An area established on non-Federal lands located within the United States or its possessions or territories for the purpose of safeguarding classified defense information or protecting DOD equipment and/or materiel. Establishment of a national defense area temporarily places such non-Federal lands under the effective control of the DOD and results only from an emergency event. The senior DOD representative at the scene will define the boundary, mark it with a physical barrier, and post warning signs. The landowner's consent and cooperation will be obtained whenever possible; however, military necessity will dictate the final decision regarding location, shape, and size of the national defense area.

National Incident Management System

A system that provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents.

Personal Identity Verification

A process to verifying a person's identity.

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 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, and locks and keys.

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 Federal Aviation Administration (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 (for example, commissary or 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.

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.

Teslin card

A type of identification card made of synthetic, waterproof material used in some DOD identification and privilege cards and also widely used for vehicle operator licenses, voter ID cards, and other forms of identification cards; for example, the DD Form 2 (United States Uniformed Services Identification Card (Retired)) and DD Form 1173 (Uniformed Services Identification and Privilege Card).