Department of the Army
United States Army Garrison
Directorate of Emergency Services
Fort Detrick, Maryland 21702-5000
06 December 2023

***Fort Detrick Regulation 190-13**

INSTALLATION ACCESS CONTROL

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 Detrick military installation. The general policies and procedures of this regulation are applicable to the National Cancer Institute (NCI) and associated contractors by negotiated host/tenant agreements.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the U.S. Army Installation Management Command (IMCOM), Headquarters (HQ), United States Army Garrison (USAG), 810 Schreider Street, Fort Detrick, Maryland 21702-5000.

Suggested Improvements. The proponent of this regulation is the Directorate of Emergency Services (DES). Readers may send comments and suggested changes on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Directorate of Emergency Services (AMIM-FDD-O), 1419 Sultan Drive, Fort Detrick, Maryland 21702-5000.

Distribution: This Regulation is distributed solely through the Fort Detrick Homepage at http://www.detrick.army.mil or Installation Extranet.

Table of Contents

* This regulation supersedes Fort Detrick Regulation 190-13, dated 21 September 2017.

Chapter 1
Introduction

1-1. Purpose

This regulation provides policy and procedures for controlling access to Fort Detrick as directed by the Senior Commander (SC) and:

a. Assists security personnel in providing a continuous appropriate level of security for Fort Detrick access control and facilitates rapid transitions to higher levels of Health/Force Protection Conditions (H/FPCON).

b. Provides standards and procedures for granting authorized personnel, vehicles, material, and denying unauthorized personnel, vehicles, and material access onto Fort Detrick.

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 Fort Detrick.

d. Addresses the minimum requirements for personnel requesting entry to Fort Detrick through established Installation Access Control Points (IACP) with a validated need to access on a recurring basis (e.g., maintenance, landscaping, construction, etc.), as well as those personnel conducting business or visiting Fort Detrick on a non-recurring or non-contract basis (e.g., taxi drivers, food delivery, friends of Fort Detrick, etc.).

1-2. General

a. Fort Detrick Army installation is defined by man-made and natural boundaries to include Area A (Main Installation), Area B, Area C (Water and Sewer Treatment Plants), and Forest Glen Annex, and is designated as a controlled access area in accordance with (IAW) Army Regulation (AR) 190-13. Installation access control is a critical aspect of the Army Physical Security Program and the Army Insider Threat Program.

b. Fort Detrick will vet personnel attempting to gain access onto the installation against authoritative U.S. Government databases, to prevent unauthorized access and detect and deter potential criminals, terrorists, or other security and insider threats.

c. Fort Detrick's access control program regulates the flow of personnel, vehicles, and materials entering and exiting the installation. It subjects all personnel and their vehicles to safety and security inspections prior to gaining access to Fort Detrick.

d. This regulation prohibits unauthorized photographing or drawings of restricted areas.

e. Inconvenience to organizations or individuals will not be a reason to circumvent or modify access control security procedures established by this regulation.

1-3. References

Appendix A lists all required and related publications and referenced forms within this regulation.

1-4. Explanation of Abbreviations and Terms

The glossary at the end of this regulation explains all abbreviations and special terms used throughout this regulation.

1-5. Records Management

Record keepers will identify, maintain, and dispose of any records created as a result of this regulation's processes IAW AR 25-400-2, The Army Records Information Management System (ARIMS), and Department of the Army Pamphlet (DA PAM) 25-403, Guide to Recordkeeping in the Army. Record titles and descriptions are available on the ARIMS website (https://www.arims.army.mil).

Chapter 2
Responsibilities

2-1. U.S. Army Garrison (USAG) Commander

a. Ensures at a minimum, access control is conducted at all operational IACPs. Provide a level of security at IACPs based on current H/FPCON Measures and/or threats to Fort Detrick 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 Fort Detrick.

c. Allocate the necessary resources to enforce established installation access control, and H/FPCON measures.

d. Maintain a visitor control program for non-DoD affiliated individuals requesting access to enter Fort Detrick.

e. Enforces the removal of, and or denies installation access to any persons who threaten the good order and discipline, health, and safety on the installation.

f. Designate restricted areas on Fort Detrick in writing for which Commanders or Directors will establish specific access control measures.

2-2. Commanders and Directors

a. Will establish, in writing, access control procedures for restricted areas as part of the units/organization/activity's Physical Security Plan (PSP) and/or Standard Operating Procedures (SOPs) within their scope of responsibility IAW AR 190-13 and this regulation.

b. Provide their PSP to the installation's Physical Security Officer (PSO) to be added as an annex to the installations PSP.

c. Appoint in writing (DD Form 577) unit/organization/activity's sponsoring authorities/Points of Contact (POC) responsible for validating access requests for contractors, vendors, service providers, or visitors pertaining to their organizational requirements or events.

d. 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.

e. Units/organization/activity's Antiterrorism Officer (ATO) and PSO hosting a special event will provide a risk assessment to the Directorate of Emergency Services (DES) for review prior to it being staffed for approval.

2-3. USAG Directorate of Emergency Services (DES)

a. Implement access control procedures for all IACPs based on current H/FPCON and local threats IAW applicable directives and this regulation.

b. Be the proponent for installation access control.

c. Control security forces and operations at all Fort Detrick IACPs.

d. Manage and implement Fort Detrick's visitor procedures.

e. Ensure Visitor Control Center (VCC) and access control personnel adhere to the requirements of this regulation.

f. Ensure authorized personnel are issued Fort Detrick passes (when authorized and applicable).

g. In coordination with unit commanders on the installation, ensure when a

family care plan is executed, the caregiver is properly vetted IAW this regulation prior to allowing access on to the installation.

h. Review all installation specific special events and provide recommendations prior to staffing.

i. Implement procedures to issue, revoke, retrieve, or turn-in federally issued ID cards or passes.

j. Will ensure the Privacy Act Statement will be conspicuously posted in the VCC and all locations where personnel ID information is being collected to conduct vetting procedures.

2-4. Director, Network Enterprise Center (NEC)

a. Provide all required communication/data lines for IACPs, VCCs, Automated Installation Entry (AIE), and Intrusion Detection Systems (IDS).

b. Provide communication functions at IACPs and VCCs in accordance with the Army Information Technology Services catalog and Service Level Agreement policy.

2-5. Public Affairs Office (PAO)

a. Will be the single POC for sponsorship of public or private non-DoD affiliated media personnel.

b. Qualified PAOs or their delegate will escort all authorized media representatives from the point of entry to exit while on Fort Detrick. Non-DoD affiliated members of the media will not be allowed unescorted access to Fort Detrick.

c. Will facilitate the dissemination of information to all stakeholders, tenants, and surrounding communities regarding changes to policy.

2-6. DoD Affiliated and Non-DoD Affiliated Personnel

a. All personnel will provide current authorized/valid identity documents IAW appendix D of this regulation and be prepared to provide required vehicle documentation when requesting access to Fort Detrick.

b. Access to Fort Detrick carries implied requirements to abide by established laws and regulations.

c. All personnel and vehicles accessing Fort Detrick are subject to safety and security inspections at any time while entering and/or on Fort Detrick.

d. Lost or misplaced AIE Card/access badges must immediately be reported to the Fort Detrick Police Desk. The VCC will only issue a replacement AIE Card/access card after receiving a lost badge memorandum which has been signed by the Fort Detrick Police Desk.

e. “Piggybacking” through any access gate is not authorized. Personnel that witness this violation must immediately report it to the Police Desk at 301-619-7114. Personnel should provide as much detail of the offender as possible such as make, model, and license plate number of the vehicle if possible. Personnel should not use physical means to challenge “piggybacking”.

f. Personnel will not “loan” their AIE card or access badges to other individuals.

Chapter 3
Policy

3-1. Policy

a. The USAG DES is the authority for granting or denying access to Fort Detrick. The Director of Emergency Services or their delegate 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.

b. Visitors will not be granted unescorted access onto Fort Detrick without verification of a need or purpose, have met required identity proofing, and have been vetted against the National Crime Information Center Interstate Identification Index (NCIC-III), the Terrorist Screening Data Base (TSDB). These requirements are detailed below.

3-2. Verification of Need or Purpose:

a. DoD CAC holders, military retirees, and military Family members have an inherent official purpose and therefore are authorized access to Fort Detrick. This inherent official purpose does not apply to “restricted access” areas on the installation, unless properly cleared.

b. Non-DoD CAC holders and non-affiliated civilians (visitors, contractors, vendors, etc.) must have a need for access validated by a Fort Detrick DoD component, unit, organization, activity, Service Member, and/or a resident for one-time, intermittent, or routine physical access to the installation. The visitor must also be sponsored by that entity.

3-3. Identity Proofing Requirements:

a. DoD CAC holders are already identity proofed and vetted to DoD personnel security

standards and are thusly granted unescorted access onto the installation. Retirees and dependents are also considered identity proofed and vetted for unescorted access.

b. If a retiree, or DOD ID card holder, wishes to gain employment on the installation as a contractor, then that person's "status" will change to a contract employee, which triggers the requirement for an employment background check and an NCIC-III check for access to the installation.

c. Contractors without a CAC will undergo an employment background check and local records check to include NCIC and the TSDB. The antiterrorism operations security coversheet for contracts also states this requirement.

d. Federal personal identity verification (PIV) credentials persons that conform to Federal Information Processing Standards Publication 201-2 (Personal Identity Verification for Federal Employees and Contractors) are considered adjudicated by Government security specialists. The PIV credential is verified upon entrance into Fort Detrick via AIE. Other requirements for access such as fitness and purpose still apply.

e. All other non-United States Government (USG) ID card applicants will provide a valid and original form of ID, which complies with Public Law 109-13 (The REAL ID Act of 2005). This is to prove identity for enrollment into AIE's database in order to issue a daily visitor's pass or AIE card. Security personnel processing an applicant will screen documents for evidence of tampering, counterfeiting, or other alteration.

3-4. Vetting Requirements:

USAG DES will oversee execution of these procedures for vetting non-DOD affiliated personnel (visitors and non-CAC eligible contractors):

a. Conduct a check of the NCIC-III and the TSDB on all non-DOD affiliated visitors 18 years of age and older to determine if the person requesting unescorted access presents a potential threat to the good order, discipline, or health and safety on the installation.

b. The USAG DES is authorized to conduct random ID checks and vetting of persons requiring access to their assigned installations, as necessary and appropriate.

c. The FBI permits the use of NCIC-III to vet non-DOD personnel for the security of military installations. The Interstate Identification Index contains automated criminal history record information. Implementation of the TSDB query is required when the capability becomes available to DOD.

(1) The USAG DES will use "QWI" with the purpose code of C when conducting NCIC-III and "persons" files checks. The QWI is an NCIC inquiry message which provides the authorized user with the capability to access both the NCIC-III (for criminal history) and NCIC persons files simultaneously with one inquiry.

(2) The NCIC persons files includes wanted persons, known or appropriately suspected terrorist (KST) list, missing person file, foreign fugitive, wanted person, gang, protection order, immigration violator, identity theft, supervised release, violent person, protective interest files and the National Sex Offender Registry.

(3) Vetting against NCIC-III is a USAG DES Department of the Army Security Guard (DASG) and/or Police function. The program must be overseen by law enforcement personnel and must conform to the requirements established in the FBI Criminal Justice Information Services (CJIS) security and specific State policy guidelines.

(4) Personnel operating NCIC terminals must comply with Maryland State policies and FBI CJIS to operate terminals. This includes but is not limited to maintaining CN1 or CN2 certification and recording all criminal history checks on a dissemination log. Personnel are required to have training related to reading and understanding NCIC-III information. They must also carry out these actions when vetting personnel:

(a) Conduct a check of records in the TSDB when available. The TSDB is the U.S. Government's authoritative consolidated database that contains terrorist identifiers concerning individuals known or reasonably suspected to be, or that have been engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism or terrorist activities.

(b) Use the adjudication standards set in this regulation to vet non-DOD affiliated personnel (visitors and uncleared contractors) and recommend disposition (allow unescorted/escorted entry, deny access and/or process for waiver).

(c) Register personnel into the AIE database while recording fitness determination decisions, date of issuance/expiration, revocation, and other information necessary to track and account for visitor processing.

(5) Personnel who have previously been vetted and issued an access card through AIE or Defense Biometric Identification System (DBIDS) can automatically be registered by presenting this same credential for access at the ACP or VCC if they provide a valid need for access.

(6) In general, AIE/Installation Access ID cards/visitor passes will coincide with the duration of the visit. AIE Badges/Installation Specific Access Badges will not be issued for more than one year or exceed the expiration date of the non-scannable CAC ID card under any circumstance. Further, the date the visitor was vetted and the purpose for being on the installation will be logged into AIE. This prevents continuous NCIC-III checks of visitors coming onto the installation within one year of the original date vetted.

3-5. Personnel Authorized Unescorted Access:

a. Personnel in lawful possession of a valid form of the following ID cards are

authorized unescorted access onto Army installations:

(1) DoD CAC.

(2) DD Form 2S (RES) (Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)); DD Form 2S (RET) Blue (United States Uniformed Services Identification Card (Retired) (Blue)); or DD Form 2S (RES RET) (United States Uniformed Services Identification Card (Reserve Retired) (Red)).

(3) DD Form 1173 (Uniformed Services Identification and Privilege Card); DD Form 1173–1 (Department of Defense Guard and Reserve Family Member Identification Card); DD Form 1173–1S (PRIV) (United States Uniformed Services Identification and Privilege Card) (Reserve Dependent) (Red); or DD Form 1173S (PRIV) (United States Uniformed Services Identification and Privilege Card (Dependent) (Tan)).

(4) DD Form 2765 (Department of Defense/Uniformed Services Identification and Privilege Card) (Tan).

(5) Retired DOD Civilian ID card.

(6) Blue striped CAC (for non-U.S. citizens). Blue striped CACs must be registered in AIE to associate the person with Fort Detrick. Newly hired foreign national personnel will be issued an AIE local pass (up to 6 months) while they wait for their CAC application to be approved.

b. Non-CAC holder contractors and vendors.

(1) Contractors and vendors requiring physical access to Fort Detrick, but who do not require access to a DoD computer network, will have a government-employee sponsor 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 Installation Access Card and/or AIE Badge will not exceed the contract date or the sponsor’s CAC expiration date, whichever occurs first. Sponsors will be held responsible for notifying the USAG DES of terminated contract employees and for turn in of expired or revoked IDs. Under no circumstance should an Installation Access Card and/or AIE card exceed one years from the date it was issued.

(2) Non-CAC eligible contractors will be issued an AIE card that will only be used for physical access onto Fort Detrick.

3-6. Other Personnel Requesting Long Term Access:

a. The personnel listed below are recognized as having a valid requirement for long-term, recurring access to Fort Detrick. The USAG DES will vet the personnel below against NCIC-III (and TSDB when available) and issue an AIE ID card for 1 year or less, or

for long term access as follows:

(1) Family care providers. Unit commanders and directors will use the family care plan per AR 600–20 to review and validate requests by Soldiers for installation access for family care providers after completion of initial identity proofing and vetting.

(2) Army volunteers. The director of an activity will review and validate requests to grant unescorted installation access for Army volunteers. They will forward the request to the senior law enforcement official after completion of initial identity proofing and vetting.

(3) Gold star Family members and next of kin survivor Family members are authorized unescorted access. The “survivor access card” will be used for both gold star Family members and next of kin survivors. The Army’s AIE system will issue an AIE card marked “Survivor.”

(a) A gold star family member is a survivor of a Service member who has lost their life during any armed hostilities in which the United States was engaged and authorized to wear the “Gold Star Lapel Button,” in accordance with AR 600– 8–22.

(b) The next of kin Family member is a survivor of a Service member who lost their life while serving on active duty.

(c) Fort Detrick’s Survivor Outreach Services (SOS) support coordinator will receive and review requests for access card(s) and verify eligibility. The SOS support coordinator will forward the request to the VCC to be vetted. When vetting is successfully completed, the survivor access card will be issued for a three-year period.

(d) This does not apply to critical sites whose mission does not allow access of unescorted non-DOD personnel, or during periods of elevated security where additional screening is required.

(4) Transportation Worker Identification Credential (TWIC) holders may be granted unescorted access to the installation after completion of identity proofing and initial vetting using NCIC-III and the TSDB and based on a valid purpose for entry to deliver commodities, provide services, or other actions approved by the commander or director. Additional documentation should be provided such as a commercial driver's license, government bill of lading, or other documentation identifying a requirement or need to enter the installation.

(5) Veteran’s Health Identification Card (VHIC) is issued to eligible Veterans by the Veteran’s Administration (VA) as a form of ID for appointments at VA care facilities. Veterans may request long-term access to the installation using the VHIC after completion of identity proofing and vetting. Three options are available if a Veteran fails to meet access control adjudication standards for unescorted access:

(a) Submit a waiver as specified in this regulation.

(b) Change to a VA Medical Clinic that is not located on the installation.

(c) Arrange to be escorted by authorized personnel.

(6) Privatized housing personnel.

(a) Balfour Beatty Communities residents will be vetted before being granted unescorted access to the installation.

(b) Balfour Beatty Communities residents that do not possess a valid DoD ID Card will be issued a two-week pass. This will assist the resident with moving into the community, while allotting sufficient time for their housing packet to be completed.

(c) Once the VCC verifies the Balfour Beatty packet they will issue the resident an AIE card and set the expiration date to coincide with their lease agreements expiration date or within one year of the NCIC-III check, whichever occurs first.

(d) Non-DOD personnel and their family members over the age of 18 that are requesting to stay in privatized lodging on Fort Detrick will be vetted against NCIC-III, in accordance with this regulation. They will be issued access based on a signed lease agreement.

(7) Non-profit, non-governmental organizations. These organizations that provide support for Soldiers and their Family members will be granted long-term access after being vetted, in accordance with this regulation.

(8) Official foreign visitors. The following official foreign visitors will be granted unescorted access and are exempt from a check of NCIC-III and TSDB records, in accordance with paragraph 8–5, unless otherwise directed by the SC or director.

(9) Official foreign visitors subject to the provisions of AR 380–10 (for example, foreign liaison officer, foreign exchange personnel, and cooperative program personnel) will be granted unescorted visitor status. The Foreign Visit System-Confirmation Module will be used to confirm that a proposed official visit by a foreign government representative has been approved through the Foreign Visit System and to record the arrival of such visitors. The module is available at https://spanweb.dtsa.mil/default.aspx.

(10) For visitors subject to the provisions of AR 12–15, the sponsoring U.S. Government office will provide documentation to the senior law enforcement official, or equivalent, that such visitors have been security screened per the policy’s requirements.

(11) Consideration for extended visitor passes, other than those stated above, are done on a-case-by-case basis. Requests must be submitted in writing by the sponsoring

Commander or Civilian equivalent and be provided to the USAG DES.

b. Search procedures and random antiterrorism measures apply to all personnel, regardless of the type of access control card they possess.

3-7. Escorted Personnel

a. Visitors who have no affiliation with the DoD and/or another federal agency located on Fort Detrick and who are not vetted in accordance with this regulation will not be granted unescorted access to Fort Detrick. They may be granted escorted access if the following requirements are met:

(1) The visitor will be escorted by authorized personnel for the duration of their visit. Authorized escort personnel may not leave visitors unattended at any point of their visit. Personnel authorized to escort visitors include uniformed Service members and spouses, DoD Civilians, CAC-holding contractors, retired Service members and spouses, and retired Civilian personnel.

(2) The visitor must possess a valid REAL ID-compliant identification document, or a valid passport from other countries cleared by the State Department and will present it to obtain escorted access.

3-8. Trusted Traveler Program

a. The purpose of a Trusted Traveler Program is to expedite access for those entering onto Fort Detrick. The program allows personnel who have a valid DoD or Government employee ID credential (CAC or PIV) to present their ID credential for access to the installation, while simultaneously vouching for occupants within their vehicle. The Fort Detrick website (https://home.army.mil/detrick/index.php/my-fort/visitors) will indicate whether this system is currently in place, and the following requirements will apply:

(1) Persons identified as trusted travelers are responsible for the actions of all occupants for whom they sponsor and for meeting all requirements for escort, as established by this regulation.

(2) The Trusted Traveler Program applies to the outermost perimeter of the installation. It does not apply to accessing facilities or areas inside the installation.

(3) Trusted travelers cannot vouch for persons with foreign passports or ID cards.

(4) Vehicle occupants that are sponsored by the trusted traveler must be 18 years of age or older and be in possession of a valid REAL ID-compliant identification document.

(5) Occupants under the age of 18 that do not possess a valid picture ID card may be sponsored by an adult occupant of the vehicle that is cleared to enter the installation.

(6) The SC or their delegate, at their discretion, may suspend the Trusted Traveler Program based on H/FPCON, local hazards and threats assessments, or may revoke individual trusted traveler privileges.

(7) DoD contractors in possession of a CAC are not authorized trusted traveler privileges.

3-9. Law Enforcement Credentials for Access to Fort Detrick During Non-Emergency Situations

a. This portion of the regulation only applies during non-emergency, non-support agreement activities. DASGs will not delay access for emergency responders operating marked emergency vehicles onto Fort Detrick during emergency situations.

b. The number of various credentials issued by agencies makes it virtually impossible for DASG at one of Fort Detrick's IACP to know if the credential is legitimate. Therefore, law enforcement credentials will not be accepted as installation access credentials by any person in civilian clothes operating an unmarked vehicle.

c. Department of the Army Civilian Police (DACP), DASG, and Firefighters assigned to USAG DES are not required to present their ID card at IACPs when they are in an official duty capacity and operating a Fort Detrick Police, Guard, or Fire department vehicle.

d. Other Federal agents must present their federally issued PIV, which can be scanned by AIE and verified against the certificate revocation list held at the Defense Manpower Data Center, as opposed to law enforcement credentials.

e. Law enforcement officials who do not have a DOD-issued CAC, a federally issued PIV, or if a DASG cannot scan or verify the PIV, will be vetted in accordance with this regulation. After initial vetting, the person can be enrolled into the AIE database by linking their driver's license as a credential, or they can be issued an AIE card.

f. Law Enforcement Officers covered under the Law Enforcement Officers Safety Act (LEOSA) are permitted to bring their personal/assigned weapon on the installation under the following circumstances:

(1) They must meet all terms outlined in the LEOSA and adhere to their agency's policies.

(2) At no point shall a LEOSA qualified officer carry any weapon in any building on the installation unless they are responding to an emergency call for service in an official capacity as a part of a law enforcement entity with the authority to carry out law enforcement duties on the installation.

(3) LEOSA qualified officers must secure their weapon inside a lockbox within their vehicle.

3-10. Special Event Access Control

a. The SC, the Director of Emergency Services, or their delegate with installation security responsibilities, will clearly define access control measures required to manage special events, circumstances, and activities on the installation.

b. The SC, the Director of Emergency Services or their delegate may waive NCIC-III vetting for personnel attending special events, activities, and circumstances, if it is impractical.

c. Units, organizations, or activities may submit vetting packets to the VCC to expedite access vetting. These packets will require name, date of birth, social security number, and reason for access. This information is considered PII and will be handled in accordance with Army regulations.

d. Compensatory security measures for special events will be implemented when the requirements of this regulation cannot be met. Examples include:

(1) Isolating event traffic and parking to specific locations or areas on the installation.

(2) Transporting attendees to and from the event site by government transportation.

(3) Directing, at a minimum, persons without a DoD/FED access control credential to the specific gate(s) where security measures are conducted prior to entrance onto the installation.

3-11. Vehicle Access

Motor vehicles (to include motorcycles) are permitted controlled entry onto Fort Detrick and must adhere to AR 190-5 requirements. Drivers must possess a valid driver’s license, vehicle insurance and state registration.

a. Access may be denied to vehicles that are obviously defective or unsafe to be operated or transported in. 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.

3-12. Bus and School Bus Access

a. For commercial busses that plan on proceeding past DASG controlled areas, DASGs will board the bus, check all IDs of personnel reasonably believed to be above the age of 18 and will ensure there is no duress situation. DASGs will validate/scan ID cards that are approved by this regulation for unescorted access onto the installation utilizing AIE handheld scanners. Prior to permitting visitor access, DASGs must validate the need to be on the installation. All personnel who fail to provide an authorized ID or valid reason to be on the installation, will disembark the bus and either go to the VCC to be vetted or be denied access to the installation.

b. DASGs will check school bus driver's license and employee identification cards prior to granting access onto the installation. They will also visually inspect the interior of the vehicle to ensure there are no signs of duress.

3-13. Instructions for Car-Sharing Service Drivers

a. All taxi drivers and ride-sharing drivers (such as Uber, Lyft, etc.) must adhere to AR 190-5. Drivers must possess a valid driver's license, vehicle insurance, and state registration.

b. Visitors, including taxi and ride-sharing vehicle drivers, must undergo identity proofing and vetting in accordance with this regulation, to determine fitness. Although drivers for ride-sharing services or taxis would then have a valid credential after proper vetting, their purpose would still need to be established for each visit, which can be accomplished by showing ride sharing/hail on a smartphone or identifying the person and location for pickup. This applies whether they present an AIE card, visitor pass, or a registered REAL ID driver's license.

c. Trusted Traveler does not apply to a ride-share driver travelling with a Service Member to enter the installation as "escorted," without going through the visitor control protocol, because they will no longer be escorted after dropping off the Service Member at the destination.

3-14. Additional Security Instructions Concerning Contractors

a. The USAG DES will continuously review Fort Detrick access control procedures, threats, H/FPCON level and ensure law enforcement, security forces, take action to prevent access by unauthorized contracted persons as follows:

(1) All contractors requesting access to Fort Detrick will be vetted to meet the requirements set by AR 525–13 and this regulation.

(2) Contractors requesting access to Fort Detrick will be vetted at either the VCC or VSA by USAG DES personnel.

b. All activities requesting access for contractors will review the contract to ensure the following is listed:

(1) Contracted workforce is compliant with all identity-verification requirements.

(2) Reason for access is validated by the requiring activity.

(3) Type of access and privileges are appropriate.

(4) Period of access is specified.

3-15. Fitness Adjudication Standards and Procedures

a. This policy describes the minimum Fort Detrick standards for controlling unescorted access to the installation. This applies to all visitors, uncleared contractors, and other persons not eligible for a CAC or other form of ID listed in this regulation. These standards provide the framework for determining the potential threat to the good order and discipline, health and safety, and fitness of such persons for unescorted access on the installation.

b. Fitness for unescorted access to Fort Detrick will be determined by an analysis of information obtained through authoritative government data sources. The sources, at a minimum, include the NCIC and TSDB (when available) to determine if granting unescorted access to a person presents a potential threat to the good order, discipline, or health and safety.

c. Unescorted access determination. The SC, in the absence of an approved waiver, may deny persons access to the installation based on information obtained from the results of a NCIC-III check, using the “QWI” under purpose code C, and the TSDB when available. These government-authoritative data source checks give an indication if a person may present a threat to the good order, discipline, and morale of the installation. This information includes, but is not limited to:

(1) NCIC-III check contains criminal arrest information about the individual that causes the SC to determine that the person presents a threat to the good order, discipline, or health and safety on the installation.

(2) The individual’s claimed identity cannot be verified based on the reasonable belief that the person submitted fraudulent identity information in attempt to gain access.

(3) There is a current arrest warrant in NCIC-III for the individual, regardless of the offense, violation, or extradition status.

(4) There is a current bar from entry or access to a federal installation or facility for the individual.

(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, or drug possession with intent to sell or distribute.

(6) The individual has been convicted of espionage, sabotage, sedition, treason, terrorism, or murder.

(7) The individual is registered as a sex offender.

(8) The individual holds a felony conviction within the last 10 years regardless of the offense or violation.

(9) The individual holds a felony conviction for a firearms or explosives violation regardless of when the conviction occurred.

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

(11) The individual has been identified in the NCIC KST file or TSDB report as known to be, or is suspected of being, a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity. Installation access control personnel will strictly follow the FBI's published engagement protocols.

d. Procedures for TSDB notifications:

(1) The KST list is derived from the TSDB, maintained by the FBI's Terrorist Screening Center (TSC). KST "hits" may be received either during initial vetting using QWI inquiry of non-DoD affiliated personnel or at installation access control points using AIE or DBIDS systems connected to Identity Matching Engine for Security and Analysis (IMESA), which checks TSDB as part of continuous vetting.

(2) DoD and FBI have jointly agreed to engagement protocols for responding to KST and/or TSDB hits. The TSC labels terrorist suspects with various handling codes. These codes will be attached to the KST-TSDB hits sent to the installation. Fort Detrick will strictly follow the handling code procedures given in the IMESA alert and response when we receive IMESA-accessed TSDB information.

(3) At no time during an encounter will the subject of a KST-TSDB hit be notified, directly or indirectly, that they are on a watch list. This procedure is key to fulfilling our responsibilities to FBI agreement for sharing KST-TSDB data with DoD. Only personnel trained and certified to access and use TSDB information (NCIC trained and certified) will be authorized to handle TSDB information in the DoD IMESA process. USAG DES must retain all personnel training records for as long as the member has access to the system and up to the period of the next audit.

(4) Following the encounter, installation access control personnel will report the incident to the Army Threat Integration Center, available 24/7 at commercial: (703) 695–5300 or Defense Switched Network: (312) 225–5300, or by email at: usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@army.mil and OPMG at usarmy.pentagon.hqda.mbx.opmg-ps@army.mil.

e. Active warrant processing.

(1) If an active warrant is identified, a warrant confirmation message (also known as a "hit" confirmation) is sent via NCIC to the agency that entered the warrant.

(2) Per system requirements, the agency must respond to the warrant confirmation response with a verification that the warrant is, or is not, active.

(3) A message from the originating agency, indicating an active warrant, will have instructions to either hold the individual or instructions to advise the individual of the warrant and release from custody. In situations where the warrant is confirmed to be active and extradition is requested, Fort Detrick police/guards will detain the individual for the law enforcement agency.

(4) Local Law Enforcement Agencies will be notified of a person(s) with an active, confirmed, in-state warrant or an out of state extraditable warrant. The USAG DES can detain any person(s) with a confirmed warrant for up to 3 hours pending the arrival and release to the extraditing agency. USAG DES will coordinate with local law enforcement agencies to ensure custody transfer.

(5) If an active warrant (security alert) is detected at an ACP, via AIE continuous vetting, in addition to the procedures listed above, installation law enforcement personnel will forward a blotter extract to the unit commander or Civilian equivalent the following morning. The unit commander or Civilian equivalent will be responsible for taking appropriate action and will ensure their Personnel Security Officer (PERSEC) is notified of the incident.

f. Installation access denial waiver process.

(1) Fort Detrick uses the following waiver process if an uncleared individual is denied access based on derogatory information obtained from an NCIC or NCIC-III check, but only if the person requests a waiver. Access control personnel will issue instructions to the denied person on how and where to submit a waiver if one is requested. The instructions will advise the person to perform the following actions:

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

(b) Obtain a letter of support from their U.S. government sponsor. The letter must

indicate that the sponsor requests that the person be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits. If a waived contractor/employee is terminated, the sponsor must inform USAG DES so that unescorted access to the installation is no longer authorized.

(c) Submit a letter requesting the access denial be waived, to the Government sponsor who will be responsible for submitting it to USAG DES for processing. The letter must include all offenses, plus an explanation why the conduct should not result in denial of access to the installation. Other factors that the sponsor and/or requesting individual should address are the:

(1) Nature and seriousness of the conduct.

(2) Specific circumstances surrounding the conduct.

(3) Length of time elapsed since the conduct.

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

(5) Current mailing address or email address for Army communications.

(d) The government sponsor will review the person's information for completeness and determine whether to endorse the request for a waiver.

(1) If the government sponsor endorses the waiver letter, he/she will provide a letter of recommendation for the person. The letter must address the relevant conduct that caused the denial and indicate why the conduct should not prohibit the person from being granted unescorted access to the installation. The government sponsor will submit the waiver packet to USAG DES for processing.

(2) The SC or their delegate will render a determination in line with the good order, discipline, health, and safety on the installation. The SC or their delegate will provide a copy of the determination to the person.

(3) The results of the SC's or delegate's decision will be provided to USAG DES to update applicable access control databases.

(4) Persons who had a waiver request denied may request reconsideration from the SC or their delegate one year after the date of the Commander's decision. Persons may request reconsideration earlier if they can present significant information that was not available at the time of the original request or show that the basis for the original denial was overturned, rescinded, or has expired.

(e) DoD or USG sponsors that knowingly sponsor an individual(s) that is

debarred from accessing Fort Detrick, is known to have an active criminal warrant or does not have a valid reason for accessing Fort Detrick may be subject to removal of sponsorship authority and administrative action as directed by the SC or their delegate.

Digitally signed by MARSH.NED.BEECHINOR.1239804736
Date: 2023.12.21 17:05:13 -05'00'

NED B. MARSH
COL, SF
Commanding

Appendix A
References

Section I
Required Publications

DoD 5200.08-R (Physical Security Program)

DoDI 2000.16 (DOD Antiterrorism Program Implementation: DOD AT Standards)

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 Resources (Sensitive and Nonsensitive))

AR 190-56 (The Army Civilian Police and Security Guard Program)

AR 525-13 (Antiterrorism)

AR 600-8-14 (Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel)

Fort Detrick Regulation 190-5 (Fort Detrick Traffic Code)

ATP 3-39.32 (Physical Security)

DTM 09-012, Incorporating Change 9 (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)

Homeland Security Presidential Directive 12 (Policy for a Common Identification Standard for Federal Employees and Contractors)

Section II
Related Publications

This section contains no entries.

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 1602 (Civilian Identification)

DA Form 2028 (Recommended Changes to Publications and Blank Forms)

DD Form 2A (Ret-Red) (Identification Card, Gray-area retirees)

DD Form 2S (Ret) (United States Uniformed Services Identification Card (Retired) (Blue))

DD Form 2S (ResRet) (United States Uniformed Services Identification Card (Reserve Retired) (Red))

DD1173-1S (PRIV) (United States Uniformed Services Identification and Privilege Card (Reserved Depenedent (Red))

DD1173S (PRIV) (United States Uniformed Services Identification and Privilege Card (Dependent) (Tan))

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

Appendix B
Sample Waiver Packet

UNCLASSIFIED

ACCESS CONTROL DENIAL
WAIVER APPLICATION

WARNING; ANY MISREPRENTATION OR OMMISSION OF INFORMATION MAY RESULT IN DENIAL OF THE REQUEST

Request Form

Please type or print neatly; attach additional sheets if necessary

1. Name (Last, First, Middle):_____ Date Of Birth _____

2. Current Address (Number and Street, City, State, Apt #, and Zip Code):

_____

3. Email address: _____

Do you want your decision emailed back to you rather than mailed to you? Yes____ No ____

4. Current Telephone Number

Home ( ) _____-_____ Work ( )_____-_____

5. Reason for requesting access to Fort Detrick: _____

6. What job has Fort Detrick offered you? _____

7. Does your job require you to have a security clearance? Yes____ No ____

8. List your **ENTIRE** Criminal History (except traffic and other infractions) as follows:

Crime(s) for which you were arrested	Crime(s) for which you were convicted (*or indicate if dismissed or nolle prosecute)*	Name and Address of court or agency	Disposition (*include sentence and conviction date*)

9. Attach a copy of all documents, certified by the Clerk of the Court, from all of your conviction(s)

10. In your own words, explain the facts of each offense and why you believe that you would not present a threat to the good order and discipline and why you should receive a waiver to the current denial. Attach additional sheets if necessary. _____

_____
_____
_____
_____

11. Explain any circumstances that lessen the seriousness of the conviction(s) and show that you have been rehabilitated. Attach additional sheets if necessary: _____

_____
_____
_____
_____

12. Have you been denied access by any other federal installation or agency? (please circle and explain)

_____Yes _____No

_____
_____
_____
_____

13. List all references that you would like the reviewing Officer to consider on your behalf. Include name, address, telephone number, and relationship

_____
_____
_____
_____
_____
_____

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

VERIFICATION

State of_____

County of_____

Under the penalty of perjury, the undersigned has examined this request for review and to the best of my abilities and belief, the above listed information is true, complete and correct

_____
Your Signature

_____
Your Printed Name

_____
Date (Month, Day, Year)

Before me, the undersigned, a Notary Public in and for said County and State, personally appeared _____ and acknowledged the execution of the foregoing instrument as his/her voluntary act and deed.

WITNESS, my hand and Notary Seal, this _____ day of _____, 20_____

_____
Notary Public, Written Signature

Figure B-1. Sample Waiver Packet Checklist

Appendix C
REAL ID ACT

1. The Real ID Act of 2005 established minimum standards for the production and issuance of State-issued driver licenses and ID cards, which include requirements for a photograph and certain biographic information, such as name, date of birth, gender, height, eye color, and address. State-issued driver licenses and ID cards from states not meeting the standards can no longer be used to access Federal facilities including Military installations unless the issuing State's compliance deadline has been extended by the Department of Homeland Security (DHS).

2. Licenses and ID cards from the Real ID non-compliant States or Territories may not be accepted without a second form.

3. Enhanced Driver Licenses (EDL): State-issued driver licenses issued in accordance with the Western Hemisphere Travel Initiative (WHTI) (WHTI) that denote identity and U.S. Citizenship and are acceptable for entry into the United States at land and Sea Ports of entry. EDL are marked as enhanced driver license and bear a small red, white, and blue US Flag logo on the front of the card. EDL from the States of Minnesota and Washington are considered more secure than Real ID Act compliant cards and can be used as the sole source for identity proofing to access Military installation. For More information on enhanced driver licenses, please visit the U.S. Customs and Border Control Website: HTTP://WWW.DHS.GOV/ENHANCED-DRIVERS-LICENSES-WHAT-ARE-THEY.

4. The most current status of State compliance with Real ID Act check can be found at: HTTP://WWW.DHS.GOV/CURRENT-STATUS-STATES-TERRITORIES.

5. The following documents are considered suitable as a second form of ID:

a. US Passport or US Passport Card.

b. PIV (Personal Identification) issued by the Federal Government.

c. PIV-I Card (Personal Identification Verification – Interoperable) issued by the Federal Government.

d. US Military ID (all members of the US Armed Forces, including Retirees and Dependent ID Card Holders and Veterans).

e. Veterans' Health Identification Card issued by the US Department of Veterans Affairs.

f. DHS "Trusted Traveler" Cards (Global Entry, Nexus, Sentri, Fast).

g. TWIC (Transportation Worker Identification Credential).

h. Merchant Mariner Card issued by DHS/United States Coast Guard (USCG).

i. Driver's License issued by the US Department of State.

j. Border Crossing Card (Form DSP-150).

k. US Certificate of Naturalization or Certificate of Citizenship (Form N-550).

l. US Permanent Resident Card/Alien Registration Receipt Card (Form I-551).

m. Foreign Passport with a Temporary (I-551) Stamp or Temporary (I-551) Printed Notation on a Machine-Readable Immigrant Visa.

n. U.S. Refugee Travel Document or other Travel Document or Evidence of Immigration Status issued by DHS Containing a Photograph (Permit to Re-Enter Form I-327 and Refugee Travel Document Form I-571).

o. Employment Authorization Document with Photograph issued by the DHS (Form I-766).

p. In the case of a Nonimmigrant Alien authorized to work for a specific employer incident to status, a Foreign Passport with a Form I-94 or Form I-94A bearing the same name as the Passport and containing an endorsement of the Aliens Nonimmigrant status, as the endorsement has not yet expired and the proposed employment is not in conflict with any Restrictions or Limitations identified on the form.

q. Identification card issued by Federal, State or local Government agencies provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.

r. US Military or Draft Record.

s. Native American Tribal photo ID.

t. Foreign Government issued Passport with a current arrival-departure record (I-Form 94) bearing the names as the same name the Passport and containing an endorsement of an Aliens Nonimmigrant status, if that status authorized the Alien to work for the employer

u. PIV-I card (Personal Identification Verification-Interoperable) issued by Non-Federal Government Entities.

6. The following documents may be deemed suitable as a second form of ID:

a. Select university, library, or school cards containing a photograph, name, and expiration date.

b. Non-Government photo identification with a person' name and address.

c. Birth certificate or document with a person's full name and date of birth.

d. Utility bill or other documentation showing the person's name and address of principal residence.

e. Vehicle registration with name and address.

Appendix D
Glossary

Section I
Abbreviations

AA&E Arms, Ammunition, and Explosives

AAFES Army and Air Force Exchange Services

ACP Access Control Point

AOR Area of Responsibility

AR Army Regulation

ARIMS Army Records Information Management System

AT Antiterrorism

BRC Basic Rider Course

CAC Common Access Card

COPS Centralized Operations Police Suite

COTR Contracting Officer's Technical Representative

COR Contracting Officer Representative

CSO Commercial Solicitation Officer

C2 Command and Control

DA Department of the Army

DACP Department of the Army Civilian Police

DA PAM Department of the Army Pamphlet

DeCA Defense Commissary Agency

DES Directorate of Emergency Services

DFMWR Directorate of Family Morale Welfare and Recreation

DHS Department of Homeland Security

DOB Date of Birth

DoD Department of Defense

DoDI Department of Defense Instruction

DoD CIO/OUSD (P&R) Department of Defense Chief Information Officer/Under Secretary of Defense (Personnel and Readiness)

DoDI Department of Defense Instruction

DPW Directorate of Public Works

DTM Directive-Type Memorandum

EACS Electronic Access Control System

EAL Entry Authorization List

ECR Entry Control Roster

ERC Experienced Riders Course

ETS Expiration, Term of Service

EXORD Execution Order

FD Fort Detrick

H/FPCON Force Protection Condition

GC Garrison Commander

GSA General Services Administration

HQDA Headquarters Department of the Army

IACP Installation Access Control Point

ID Identification

IMCOM Installation Management Command

IAW In Accordance With

IDS Intrusion Detection System

IET Initial Entry Training

KO Contracting Officer

LEOSA Law Enforcement Officers Safety Act

LRC Logistics Readiness Center

METS Mission Essential Tier System

MG Major General

MS Medical Staff

MEVA Mission Essential or Vulnerable Area

MSF Motorcycle Safety Foundation

NAF Non-Appropriated Funds

NFGTSA Nallin Farm Gate Truck Search Area

NCI National Cancer Institute

NCIC-III National Crime Information Center Interstate Identification Index

NCOIC Noncommissioned Officer in Charge

NEC Network Enterprise Center

NTE Not to Exceed

OCONUS Outside Continental United States

PAO Public Affairs Office

PCS Permanent Change of Station

PIV Personal Identification Verification

PIV-I Personal Identification Verification-Interoperable

PKI Public-Key Infrastructure

POC Point of Contact

POV Privately Owned Vehicle

PRP Personnel Reliability Program

RAM(P) Random Antiterrorism Measures (Program)

SC Senior Commander

SCIC State Crime Information Center

SOP Standing Operating Procedure

TWIC Transportation Worker Identification Credential

UFC Unified Facilities Criteria

USCG Unites Coast Guard

USG United States Government

VA Veterans Administration

VCC Visitor Control Center

VIN Vehicle Identification Number

VIP Very Important Person

VRS Vehicle Registration System

Appendix E
Terms

Access control Permitting/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.

Army Standard for Access Control Points Provides standards for Army ACPs.

Army Standard (Part I) and System Specifications (Part II) for Automated Installation Entry Provides standards for Army AIE.

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 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.

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).

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.

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 Entry Control Roster (ECR) and Electronic Access Control System (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.

Facility Any single building, project, or site.

Force Protection Conditions See AR 525-13.

Fort Detrick Installation Access Badge. An approval pass that issued by the Visitor Control Center (VCC) for access to the Installation for 30 days or less.

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.

Law Enforcement Officers Safety Act (LEOSA) H.R.218 was enacted into public law and allows qualified law enforcement officers or qualified retired law enforcement officers, notwithstanding any other provision of the law of any State or any political subdivision thereof, to carry a concealed firearm and are not subject to concealed carry laws of any state.

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 ECR signed by the controlling authority (installation/activity commander) or who have been enrolled in an 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 un-cleared personnel with a need for entry into the limited area.

Media All Television, Radio, Internet, and other news reporting employees. Media shall be escorted at all times by a representative of the Public Affairs Office.

Mission Essential or 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.

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.

Non-Official Foreign Visitors Are those foreign visitors who are being utilized by contractor companies as laborers, visitors being escorted to eating establishments, Directorate of Family and Morale, Welfare and Recreation activities, etc.

Non-Official Visitor Any visitor to Fort Detrick who does not have official business with the US Army or federal government elements. This includes non-contractor vendors and suppliers, visitors to family housing areas, salvage buyers, etc.

Official Foreign Visitors Any foreign national or US citizen who represents a foreign government or business entering or seeking to enter Fort Detrick, and whose visit has been coordinated through the US State Department and appropriate Army channels.

Official Visitor A visitor who has official business with DoD or federal organizations and/or activities within the scope of this regulation. Such visitors include military and civilian DoD officials, DoD contractor officials and employees, etc.

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 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.

Preregistration Registration of visitors, official or non-official, prior to their expected visit. This should be conducted 24 hours in advance for groups of visitors consisting of 5 or less personnel. Groups of visitors consisting of 6 to 50 personnel should be coordinated at least 72 hours in advance. Groups of visitors consisting of 51 or more personnel should be coordinated at least two weeks in advance

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.

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.

Visitors Pass Approval A pass that issued by the Visitor Control Center (VCC) for access to the Installation for 30 days or less.