Headquarters
United States Army Europe and Africa
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command
Europe
Wiesbaden, Germany

Headquarters
U.S. Naval Forces Europe/U.S. Naval Forces Africa/
U.S. Sixth Fleet
Naples, Italy

Headquarters
United States Air Forces in Europe/
United States Air Forces Africa
Ramstein, Germany

Army in Europe and Africa
Regulation 190-16*

CNE-CNA-C6F/CNREURAFCENT
Instruction 5530.1

USAFE-AFAFRICA
Instruction 31-207

12 April 2024

Military Police

Installation Access Control for the U.S. Forces in Europe

***This publication supersedes AE Regulation 190-16, 27 April 2017;**
rescinds AE Form 190-16B, AE Form 190-16C, AE Form 190-16H, and AE Form 190-16I;
and rescinds AEA Command Memorandum 2022-005, 5 May 2022.

For the Commander:

MICHAEL D. WICKMAN
Major General, GS
Chief of Staff

Official:

SCOTT T. CHANCELLOR
Chief, Document Management
Army in Europe and Africa

Summary. This publication prescribes access control policy and procedures for U.S. Forces installations in the United States European Command (USEUCOM) area of responsibility (AOR). It does not apply to controlled areas governed by regulations that are more restrictive. Violations of the provisions in this publication may subject individuals to adverse administrative or civilian misconduct action.

Summary of Change. This revision—

● Initiates a joint Service publication for more consistent access control at U.S. Forces installations in the USEUCOM AOR.

● Makes changes throughout to incorporate the upgrade of the "Installation Access Control System (IACS)" (glossary) from Defense Biometric Identification System (DBIDS), version 3, to DBIDS, version 5, as outlined in AEA Command Memorandum 2022-005, which is hereby rescinded.

● Rescinds the following Army in Europe (AE) forms:

○ AE Form 190-16B, Receipt for Confiscated ID Card.

○ AE Form 190-16C, Record of Destruction.

○ AE Form 190-16H, Installation Access Control System (IACS) Deny Access Letter.

○ AE Form 190-16I, Installation Access Control System (IACS) Accept Access Letter.

● Makes administrative changes throughout (for example, phone numbers, email addresses, office symbols).

Applicability. This publication applies to persons requiring access to U.S. Forces-controlled installations in Europe. It is not intended to restrict the authority of U.S. or host nation commanders of contingency bases or bases operating in austere environments, but to standardize access control as much as possible in using the IACS.

Records Management. Records created as a result of processes prescribed by this publication must be—

● Identified, maintained, and disposed of by Army in Europe and Africa units according to AR 25-400-2. Record titles and descriptions are provided in the Army Records Information Management System at *https://www.arims.army.mil*.

● Identified, maintained, and disposed of by CNREURAFCENT organizations according to Navy records management policy.

● Maintained by USAFE/AFAFRICA units in accordance with AFI 33-322 and disposed of in accordance with the Air Force Records Disposition Schedule in the Air Force Records Information Management System at *https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm*.

Supplementation. "Area commanders" (glossary) may develop policy and procedures that meet or exceed the standards of this publication to meet their unique needs.

Forms. This publication prescribes AEA Form 190-16A, AEA Form 190-16E, AEA Form 190-16F, AEA Form 190-16G, and AEA Form 190-16K. AEA and higher level forms are available on the Army in Europe and Africa Publications (AEPUBS) website at *https://intranet.eur.army.mil/aepubs/*.

Proponency. The proponent of this publication is the IACS Program Office, Office of the Provost Marshal, G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF (mil 314-537-2264). Users may send comments and suggested improvements to the policy in publication by email to *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil*.

Distribution. This publication is available on AEPUBS at *https://intranet.eur.army.mil/aepubs/*.

CONTENTS

SECTION I
GENERAL

1. PURPOSE
This publication—

a. Prescribes policy, responsibilities, and procedures for granting access to U.S. Forces installations in Europe using the “Installation Access Control System (IACS)” (glossary).

b. Provides registration procedures.

c. Provides procedures for preparing and issuing “installation passes” (glossary).

d. Must be used with applicable Service or “component” (glossary) publications.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. GENERAL

a. U.S., host nation (HN), and NATO installations used by the U.S. Forces in the United States European Command (USEUCOM) area of responsibility (AOR) are restricted areas. Access control to these installations is essential to protecting assets and personnel from unlawful acts. These acts include, but are not limited to criminal, terrorist, and foreign intelligence threats. The proper identification, vetting, and control of authorized individuals are keys to maintaining safe and secure installations. Only authorized individuals as described by this publication may be granted access. This publication prescribes installation access control policy and provides procedures for personnel vetting and verification.

b. Department of Defense Manual (DODM) 5200.08, Volume 3, policies apply to all DOD installations located in the United States (including the continental United States, Alaska, Hawaii, Puerto Rico, and Guam). This publication meets the intent of the DODM and corresponding Service regulations for access to U.S. Forces installations located outside the continental United States (OCONUS), as permitted by applicable HN agreements, status of forces agreements (SOFAs), and other requirements.

c. This publication standardizes USEUCOM installation access control at installations that use the IACS and is based on the following component regulations for access to OCONUS U.S. Forces installations:

(1) AR 190-13, The Army Physical Security Program.

(2) AFMAN 31-101V3, Installation Perimeter Access Control.

(3) CNIC-M 5530.2, Navy Installation Access Control.

d. The IACS provides—

(1) An additional layer of security by electronically authenticating installation access for authorized individuals and denying access to individuals identified as unfit for installation access (for example, individuals who are barred, are on a watch list, are wanted by law enforcement (LE), or are using a stolen or lost DOD ID card).

(2) The ability to implement force protection measures across USAREUR-AF, CNREURAFCENT, and USAFE/AFAFRICA, or at the garrison or installation level based on the force protection condition (FPCON).

(3) Centralized control of access privileges. (For example, sponsors may withdraw the access authorization of a terminated employee; commanders may bar individuals; the “military police (MP)” (glossary) desk may flag individual IACS records.)

e. Individual access privileges are risk-based and depend on an individual's installation pass "category" (glossary) and ID card type.

f. For the purpose of this publication, the terms below are standardized as follows:

(1) A gate to an installation is called an "access control point (ACP)" (glossary).

(2) Military LE personnel, including security forces and masters-at-arms, are called "military police (MP)."

(3) United States Army garrison (USAG) commanders, USAFE/AFAFRICA commanders, CNREURAFCENT commanders, and HN commanders (as applicable, based on agreements between the United States and HNs) are called "area commanders" (glossary).

5. AUTHORITY

USEUCOM Antiterrorism (AT) Operation Order (OPORD) 23-01 designates USAREUR-AF as the USEUCOM proponent for—

a. Installation access control policy.

b. The USEUCOM Watchlist.

c. The Joint Installation Access Working Group (JIAWG).

6. RESPONSIBILITIES

a. USAREUR-AF G2. The USAREUR-AF G2 will manage the German "Local National Screening Program (LNSP)" (glossary) in accordance with AEA Reg 604-1.

b. USAREUR-AF G3. The USAREUR-AF G3 will coordinate changes to—

(1) AEA Reg 525-13 concerning installation access during elevated FPCONs.

(2) AEA Reg 525-50 concerning installation access for inspection teams.

c. USAREUR-AF G6. The USAREUR-AF G6 will provide an automated online system to support the LNSP.

d. USAREUR-AF Provost Marshal (PM). As the USAREUR-AF proponent for access control, the PM will—

(1) Serve as the Executive Agent to the USEUCOM JIAWG. The PM will lead the JIAWG to ensure that consistent and coordinated installation access control processes and policies are implemented throughout the USEUCOM AOR where the IACS is used.

(2) Develop and coordinate access control policy and procedures affecting U.S. Forces members in the USEUCOM AOR with the JIAWG.

(3) Serve as the approving authority for written requests for exception to policy (ETP) to this publication submitted to the JIAWG, and will incorporate permanent changes resulting from approved exceptions into the next revision of this publication as applicable.

(4) Appoint a USEUCOM Access Control Program Manager (e below). The Program Manager will be the USEUCOM Primary Base Security Officer (BSO).

e. USEUCOM Access Control Program Manager. The USEUCOM Access Control Program Manager will—

(1) Manage the JIAWG, which includes organizing and running the JIAWG, and will elevate policies and issues to the USEUCOM J34 for decision or action.

(2) Enter installation commander bars into the IACS.

(3) Provide policy clarification and direction for installation access control.

(4) Conduct staff assistance visits (SAVs) to review IACS registration and installation pass issuing operations and procedures.

(5) Ensure that all "installation access control offices (IACOs)" (glossary) comply with regulatory requirements.

(6) Perform audits on IACS user activity to identify deviations from policy and violations of law (for example, violations of the Privacy Act of 1974, violations of "European Union (EU)" (glossary) and HN privacy laws).

(7) Maintain and update the USEUCOM Watchlist.

f. USAFE/AFAFRICA A4S. The USAFE/AFAFRICA A4S will—

(1) Serve as the USAFE/AFAFRICA Executive Agent to the USEUCOM JIAWG and will coordinate with the USAREUR-AF PM on installation access control processes and policies.

(2) Appoint a USAFE/AFAFRICA Access Control Program Manager. The Program Manager will—

(a) Serve as the USAFE/AFAFRICA Primary BSO.

(b) Participate in the JIAWG and elevate policies and issues that the JIAWG is unable to resolve to USEUCOM J34 for decision or action.

(c) Provide policy clarification and direction on installation access control to USAFE/AFAFRICA installations.

(d) Review and approve or deny single-instance ETP requests for individuals or situations.

(e) Conduct USAFE/AFAFRICA SAVs to review IACS registration and installation pass issuing operations and procedures to ensure that all IACOs comply with regulatory requirements.

g. CNREURAFCENT N34. The CNREURAFCENT N34 will—

(1) Serve as the CNREURAFCENT Executive Agent to the USEUCOM JIAWG and will coordinate with the USAREUR-AF PM on installation access control processes and polices.

(2) Appoint a CNREURAFCENT Access Control Program Manager. The Program Manager will—

(a) Serve as the CNREURAFCENT Primary BSO.

(b) Participate in the JIAWG and elevate policies and issues that the JIAWG is unable to resolve to USEUCOM J34 for decision or action.

(c) Provide policy clarification and direction on installation access control to Navy installations.

(d) Review and approve or deny single-instance ETP requests for individuals or situations.

(e) Conduct CNREURAFCENT SAVs to review IACS registration and installation pass issuing operations and procedures to ensure that all IACOs comply with regulatory requirements.

h. Area Commanders.

(1) Area commanders will—

(a) Develop policy to ensure that access to installations within their AOR is controlled in accordance with this publication.

(b) Incorporate installation access control policy into organizational inspection programs.

(c) Establish procedures for coordinating with sponsoring organizations to determine access authorization for installation pass “applicants” (glossary) when the results of the background check include adverse information.

(d) Serve as senior officials for making fitness determinations and adjudicating an individual’s access in accordance with appendix E when the background check reveals adverse information. Area commanders may designate personnel in writing to make fitness determinations. They may also develop policy to either accept another area commander’s adjudication recommendation or initiate their own adjudication process.

(e) Review and approve or deny single-instance ETPs for individuals or situations.

(f) Serve as the adjudication authority for requests for “redress” (glossary) of access denial (AEA Form 190-16G).

(g) Notify the USEUCOM Installation Access Control Program (IACP) Manager by email (usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil) of all debarments.

(h) Perform sponsoring responsibilities as designated.

(i) Consult the JIAWG on access options when the access requirements in paragraph 9 do not adequately support co-use agreements with the HN.

(2) Area commanders may need to adapt the policy and procedures in this publication to meet unique HN laws and agreements. Changes must meet or exceed the security standards and intent of this publication whenever possible.

i. Area Commanders in the Benelux, Bulgaria, Italy, Poland, Romania, and the United Kingdom. In addition to performing the responsibilities in subparagraph h above, these area commanders will—

(1) Adapt the policy and procedures in this publication to satisfy applicable HN laws and other provisions included in U.S.–HN agreements (for example, requirements for background checks, obtaining fingerprints, residence and work permits). The adapted policy and procedures will meet or exceed the security standards and intent of this publication whenever possible.

(2) Notify the JIAWG of approved policy measures.

j. Directors of Emergency Services (DESs), Security Forces Squadron (SFS) Commanders, and Installation Security Officers (SECOs). DESs, SFS commanders, and installation SECOs will—

(1) Nominate a primary and an alternate installation BSO to the component (that is, to the USAREUR-AF OPM, the USAFE/AFAFRICA A4, or the CNREURAFCENT C3).

(2) Ensure IACS users are authorized and removed from the IACS software using DD Form 2875. DD Form 2875 will be posted to a central portal per component policy.

(3) Enforce removal of "visitor sponsor privileges" (glossary) for violating the physical escort policy (para 29d).

(4) Ensure that every ACP has an adequate supply of the appropriate confiscation form (for example, DA Form 4137) and of AEA Form 190-16G, and paper and toner for printing the escorted visitor paper pass.

(5) Ensure that all IACS users, including sponsors, complete training as required per component policy.

(6) Ensure that procedures are in place to confiscate installation passes or DOD ID cards from individuals who no longer require installation access or have an "unserviceable" (glossary) or expired installation pass or DOD ID card.

(7) Ensure that ACP guards provide the appropriate confiscation forms when an installation pass or DOD ID card is confiscated. MP Soldiers will regularly collect and return the installation passes or DOD ID cards to the appropriate office for processing and destruction.

k. Contracting Offices. Contracting offices awarding contracts that require access to U.S. Forces-controlled installations will—

(1) Ensure that contracts include requirements for background checks and, if necessary, for valid residence and work permits required for issuing installation passes or for entering individuals on "access rosters" (glossary) in accordance with this publication.

(2) Include a provision in contracts to ensure that "contractors" (glossary) return all installation passes to the issuing IACO when the contract is completed or when a contracted employee no longer requires access (for example, when the employee resigns or is terminated).

(3) Develop procedures for contracting officer's representatives (CORs), alternate contracting officer's representatives (ACORs), and their representatives to ensure that requiring activities requesting contract services include the required information on all purchase requests and commitments (PR&Cs) (DA Form 3953), military interdepartmental purchase requests (MIPRs) (DD Form 448), and other requests for contracting support when the contract will result in contractors requiring access to U.S. Forces installations.

(4) Ensure that CORs, ACORs, and their representatives inform the responsible IACO when a contractor common access card (CAC) is revoked before its expiration date (for example, when contractor employment is terminated or contract services were completed ahead of schedule).

(5) Ensure that CORs, ACORs, and their representatives turn in expired or revoked contractor CACs to the nearest Defense Enrollment Eligibility Reporting System (DEERS)/Real-Time Automated Personnel Identification System (RAPIDS) office.

l. IACOs. Paragraph 10 explains IACO responsibilities.

m. Sponsoring Organizations and Individuals. Sponsoring organizations and individuals will ensure that—

(1) Sponsored persons have a legitimate requirement to enter an installation.

(2) An installation pass "application" (glossary) (AEA Form 190-16A) is prepared for each applicant. The application will identify an applicant's access requirements and justify these requirements in accordance with this publication (for example, requirements for being granted visitor sponsor privileges). Failure to provide sufficient justification on the application may result in privileges being denied or the application being rejected.

(3) Applicable background checks are initiated and completed and appropriate actions are taken based on the results. When any adverse information is discovered, the sponsoring organization must coordinate with the area commander.

(4) Issued installation passes are retrieved and returned to the issuing IACO when they are no longer authorized or when an individual's employment is terminated.

(5) The local IACO is informed when a CAC issued to a NATO member, a non-U.S. military member, or a local national (LN) employee is revoked before its expiration date.

(6) Blue-stripe CACs issued to non-U.S. persons (for example, NATO members, non-U.S. military members, LN employees) that have expired or were revoked are turned in to the nearest DEERS/RAPIDS office.

(7) A record of personnel sponsored by the organization and supporting documentation are maintained.

(8) A reconciliation of installation passes is conducted with the servicing IACO every 6 months to verify that all sponsored individuals still require installation access and that all data and access requirements are current. Failure to complete the reconciliation will result in all sponsored individuals losing installation access.

(9) DD Forms 577 that designate persons authorized to perform "sponsoring official" (glossary) duties on behalf of the sponsoring organization (para 12a(2)(a)) are sent to the servicing IACO and are valid until revoked.

(10) The procedures in paragraph 12b(8) are followed when the sponsoring official cannot escort an applicant to the servicing IACO.

(11) They complete training to qualify as sponsors as required based on the IACS card category for which they serve as sponsors. USAREUR-AF sponsors must complete the training once and must confirm their continuing status as sponsors annually by email.

(12) Personally identifiable information (PII) is protected against unauthorized access and that its release is restricted based on a need to know (for example, for access control screening requirements, for law enforcement purposes).

n. Individuals Requiring Access to U.S. Forces Installations. These individuals will—

(1) Consent to the procedures for obtaining digitized fingerprint minutia data (DFMD) in accordance with applicable agreements with the HN.

(2) Request an installation pass if they do not have an authorized DOD ID card and require recurring unescorted access to U.S. Forces-controlled installations in Europe. The installation pass may be issued only after the proper documentation has been submitted to the servicing IACO.

(3) Carry their DOD ID card or installation pass when on a U.S. Forces installation. On request, they will present their DOD ID card or installation pass to the MP or guards. Refusal to present their DOD ID card or installation pass may be grounds for administrative or punitive action.

(4) Immediately report a lost or stolen DOD ID card or installation pass to the MP office.

(5) Inform the sponsoring organization of any change to the official relationship that serves as the basis for installation access.

(6) Turn in their installation pass to the servicing IACO or sponsoring organization when the pass expires or when the basis for obtaining the pass no longer exists.

7. POLICY

Area commanders are responsible for the security of their installations and for ensuring that the requirements of this publication are enforced. Inconvenience to individuals is not a valid reason for circumventing or modifying the procedures established in this publication.

8. EXCEPTIONS TO POLICY

a. The USAREUR-AF PM may approve ETPs for up to 1 year.

b. Requests for an exception to any policy or procedure in this publication must be sent through appropriate command channels to the JIAWG at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil*.

c. Area commanders or their designees may approve ETPs as stated in paragraph 6h(1)(e) and as authorized elsewhere in this publication.

SECTION II
INSTALLATION ACCESS PROCEDURES

9. ACCESS REQUIREMENTS

a. Persons may be authorized access to U.S. Forces installations if any of the following applies:

(1) They possess a valid DOD ID card.

(2) They possess a valid installation pass (fig 1).

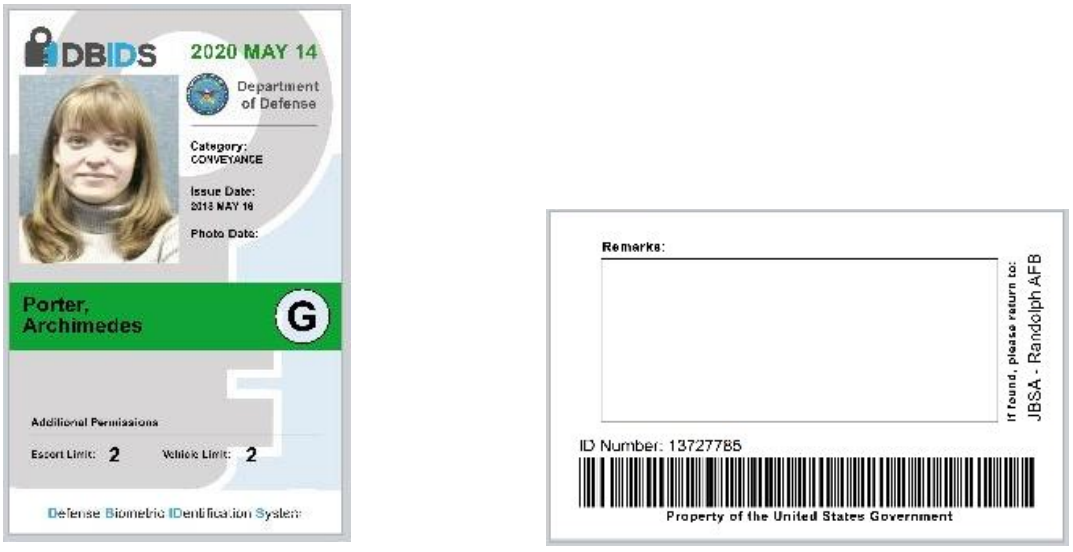

Figure 1. Sample Installation Pass

(3) They are physically escorted by an individual with visitor sponsor privileges and present one of the following identification documents:

(a) International passport.

(b) “European Economic Area (EEA)” (glossary) national ID card issued by the country of citizenship (for example, the *Personalausweis* in Germany, the “*Identiteitskaart*” (glossary) or “*carte d’identité*” (glossary) in Belgium, the “*carta d’identità*” (glossary) in Italy).

(c) NATO ID card (Allied Command Operations or Allied Command Transformation Mission Identification System ID card).

(d) HN military ID card.

(e) HN government official ID card (for example, *Dienstausweis* in Germany).

(f) HN police ID card (for example, *Polizeidienstausweis* in Germany).

(4) They are on an approved access roster and present one of the documents listed in (3)(a) through (f) above.

b. There may be situations when area commanders must supplement the requirements in subparagraph a above for operational reasons (for example, large-scale training exercises that involve non-U.S. military members, running formations during organized unit physical training, military convoys). Exceptions to the requirements in subparagraph a above must be defined in installation policy and approved by the area commander.

c. Refugees, asylum seekers, and stateless persons who have been issued a travel document are not authorized an installation pass, a visitor paper pass, or placement on an access roster. Most travel documents have two black stripes in the top left corner of the HN-issued document and the words “Travel Document” printed in English, French, and the HN language on the front. With prior coordination, area commanders may approve ETPs for their installations on a case-by-case basis (for example, for visiting immediate Family members).

d. Individuals issued an *Ersatz-Personalausweis* (a replacement German national ID card) by the German Government are ineligible for an installation pass, a visitor paper pass, and placement on an installation access roster. The *Ersatz-Personalausweis* looks similar to a *Personalausweis*, and when presented as an ID document, all guards and “registrars” (glossary) will deny access and will contact the MP desk and provide details of the encounter. The DES, SFS commander, or SECO will report the encounter using the SPOT report. On 30 June 2015, the German Government began issuing an *Ersatz-Personalausweis* as a replacement ID document (replacing a *Personalausweis* or a *Reisepass* (passport)) to individuals identified as extreme Islamists, as required by the UN Security Council Resolution 2178 of 24 September 2014.

e. Citizens from countries identified by the U.S. Department of State as state sponsors of terrorism (*http://www.state.gov/j/ct/list/c14151.htm*) require area commander approval to access installations. These individuals must not be placed on an access roster. The sponsor will send a request for installation access through the responsible security office for preparation of a recommendation to the area commander. Guidance follows the U.S. Department of State requirement for an additional screening of citizens from identified countries before these individuals are granted entry into the United States (Immigration and Nationality Act, 8 USC 1101(a)(15), and Section 306 of the Enhanced Border Security and Visa Reform Act of 2002).

f. Paragraph 31 prescribes policy for emergency vehicle access; paragraph 32 for special vehicle access; and paragraph 33 for coordinated access.

g. Persons such as a refugees who request U.S. asylum or refuge on a U.S. installation are denied access and should be referred to the U.S. embassy or consulate in the HN. The only exception is temporary refuge, which may be granted if the person's life or safety is in imminent danger (AR 550-1).

h. Area commanders will not further restrict access unless a bona fide need exists (for example, if an installation has critical assets or restricted areas and no other layers of protection are available). In these situations, area commanders may determine that additional documents (for example, a special pass) are required to gain access to their installations. Area commanders are not authorized, however, to use these alternative access documents in place of DOD ID cards or installation passes.

10. INSTALLATION ACCESS CONTROL OFFICES

a. Area commanders are responsible for the security of their installations. Therefore, access control is an area commander's responsibility. They may approve short-term ETPs after making a risk-based assessment and determining that they are willing to accept the risk based on the situation and circumstances.

b. Components will functionally align their IACOs under the unit or organization that is responsible for physical security.

c. Only approved registrars are authorized to issue passes. Registrars will—

(1) Report all incidents involving false information or manipulation to the MP.

(2) Develop a system to reconcile with each sponsoring organization every 6 months to ensure that sponsored individuals still require the same level of installation access.

SECTION III
INSTALLATION ACCESS FOR DOD ID CARDHOLDERS

11. TYPES OF IACS REGISTRATION

There are two types of IACS registration: implicit and explicit.

a. Implicit Registration at ACPs. Most DOD ID cards will be implicitly registered when scanned by the ACP guard. The IACS will confirm that the DOD ID is a current ID with no derogatory flags and will allow access at those ACPs that are not restricted.

b. Explicit Registration of ID Cards at IACOs. The following ID cards will be registered at IACOs:

(1) DOD Blue-Stripe CAC. Non-U.S. citizens who have been issued a CAC with a blue stripe will be registered in IACS with the corresponding privileges and restrictions as specified by AEA Form 190-16A:

(a) Foreign Government Civilian/Local National Employee (para 19).

(b) Foreign Government Contractor (para 20).

(c) Foreign Military/Foreign Military Dependent (para 21).

(2) Veterans Health Identification Card (VHIC). VHICs may be registered in IACS in Germany if approved by the area commander based on shopping, MWR availability, and mission requirements. The VHIC (fig 2) is issued to veterans by the U.S. Department of Veterans Affairs (VA). IACOs may register the VHIC in IACS or issue primary or Family caregivers an installation pass in the "Conveyance" category (para 16) if the following requirements are met:

Figure 2. Sample Veterans Health Identification Card

(a) Eligibility Check: Veterans must present their VHIC (fig 2) to the registrar who will verify that one of the following eligibility statuses is listed: Purple Heart, Medal of Honor Recipient, Former Prisoner of War, Service Connected Disability. Primary and Family caregivers (also known as shopping assistants) must present their VA eligibility letter.

(b) Installation Access: Access may be granted to the installation (or installations) that is closest to the veteran's residence and that has facilities that the veteran is authorized to use (for example, PX or BX, commissary, MWR facilities).

(c) Background Checks:

1. Good Conduct Certificate (GCC) for veterans residing OCONUS.

2. U.S. National Crime Information Center (NCIC) check.

3. LNSP screening for veterans residing in Germany.

4. Carabinieri check for veterans residing in Italy.

(d) Visitor Sponsor Privileges: Not authorized.

(e) Authorized Days and Times: 24 hours a day, 7 days a week (24/7).

(f) FPCON Restriction: Bravo.

(g) Residence Permit: Required for registrations of more than 90 days for non-EU residents.

(3) DOD ID Cards Causing Access Denial When Scanned. Not all DOD ID cards are implicitly registered in IACS. Individuals with DOD ID cards identified as having insufficient permissions when scanned can make an appointment with the IACO to request installation access. These individuals are authorized to sponsor themselves and Family members with DOD ID cards. Using AEA Form 190-16A, they must provide the purpose and a justification for access, and the dates and times for which access is requested. The area commander or the commander's designee will review and approve or disapprove the request.

(a) Days and Times Access is Authorized: 24/7.

(b) FPCON Restriction: Bravo.

(c) Residence Permit: Required for registrations of more than 90 days for non-EU residents.

SECTION IV
ISSUANCE OF AN INSTALLATION PASS

12. APPLICATION PROCESS

a. Key Components. The application process includes the following key components:

(1) Sponsoring Organization. The sponsoring organization will designate individuals within the organization to carry out sponsoring organization responsibilities. The sponsoring organization for each applicant is based on the applicant's installation pass category. For example, area commanders and their IACOs will serve as sponsoring organizations for some applicants, and hiring organizations will serve as sponsoring organizations for other applicants.

(2) Sponsoring Official. The sponsoring official is key to the integrity of the IACP. Sponsors will complete the IACS sponsorship training before approving access requests.

(a) Sponsors of installation pass applicants will be designated in writing using DD Form 577.

(b) DD Form 577 requires specific information in the following blocks:

1. Block 6: Check "DEPARTMENTAL ACCOUNTABLE OFFICIAL."

2. Block 7: Enter "Authorizing Official for IACS Installation Pass and for registering DOD CACs in IACS."

3. Block 8: Enter "AEA Reg 190-16."

(c) Sponsoring organizations will send approved DD Forms 577 to the local IACO.

(d) IACOs will review DD Forms 577 to verify the sponsor's authority and will reject all applications signed by unauthorized individuals.

(e) The following are minimum grade requirements for sponsoring officials and limits to their approving authority:

1. Supervisors in the grades of O-1, E-7, W-2, GS-9, NF-3, C6A, or above are authorized to sponsor individuals for single-installation access only.

2. Supervisors in the grades of O-3, E-8, W-3, GS-11, NF-4, C7, or above are authorized to sponsor individuals for access to installations within an area commander's AOR.

3. Supervisors in the grades of O-5, GS-13, NF-5, C8, or above are authorized to sponsor individuals for component-wide (USAREUR-AF, USAFE/AFAFRICA, or CNREURAFCENT) access.

4. Area commanders or their designees may grant an ETP if an organization is unable to meet the grade requirements.

5. There are no grade restrictions for CORs, ACORs, site contracting officer's representatives (SCORs), or appointed contractor representatives when sponsoring personnel that are on their contracts. Grade restrictions do apply when sponsoring other individuals that are not on their contracts.

6. Installations in the Benelux, Bulgaria, Italy, Poland, Romania, and the United Kingdom must use equivalent pay grade structures for their LN employees.

(f) NATO Sending States and the United States Mission, Germany, will submit DD Forms 577 to the OPM to post on the USAREUR-AF IACS portal. IACOs will honor any DD Form 577 posted on the USAREUR-AF IACS portal.

(3) Category. An applicant's category will determine the type of pass that may be issued and the associated restrictions. Sponsoring officials will select the category on AEA Form 190-16A, and registrars will verify its correctness. Registration requirements and restrictions vary among the different categories.

(4) Background Checks.

(a) Background checks are required to determine the "fitness" of a person requesting installation access. "Fitness" includes both character and conduct of an individual. Appendix E provides fitness standards for unescorted access through which an individual's fitness is determined. Sponsoring organizations are responsible for initiating required background checks and for ensuring that background checks are completed. They should refer to the appropriate pass category (paras 16 through 28) to determine the background check requirements for each applicant. Registrars are responsible for verifying that a background check has been completed or initiated if necessary. The types of background checks are as follows:

1. GCC. Applicants will obtain this certificate from their local registration office (for example, from the town hall, the municipal office, the citizens' registration office (*Meldebehörde* in Germany)). A certified translation must be obtained for all GCCs that are not completed in English, German, or Italian. Certificates that are older than 12 months may not be used. If an individual is unable to get a GCC in the current country of residence (for example, if the individual has resided less than 1 year in that country), an equivalent certificate is required from the previous country of residence. That document must be translated into English and notarized.

2. U.S. Security Check. U.S. security checks are conducted only on U.S. citizens and permanent residents. U.S. security checks include all authorized databases that are available to screen an applicant (for example, National Crime Information Center Interstate Identification Index (NCIC III) for non-DOD-affiliated individuals, the Army Law Enforcement Reporting Tracking System (ALERTS), the Security Forces Management Information System (SFMIS)).

3. HN Federal Background Check. An HN federal background check, if available, is required both for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. Sponsoring organizations will comply with LNSP procedures in AEA Reg 604-1. IACS registrars will log on to the LNSP website to confirm LNSP background check initiation and completion. Questions about the LNSP should be addressed to the unit or organization security officer.

a. In Germany, sponsors will monitor LNSP results every 30 days. After 90 days, if LNSP results have not been received, they will contact the LNSP office at the Office of the Deputy Chief of Staff, G2, HQ USAREUR-AF (*usarmy.wiesbaden.usareur.list.g2-isd-sso-lnsp@army.mil*), to check on the status. Sponsoring officials will notify the IACO by email when an LNSP background check has been completed.

b. Once an HN background check has been completed (without entries), the applicant's record will be updated.

NOTE: Individuals with a DOD CAC or a Secret or higher clearance are already vetted and are exempt from any further background checks (for example, GCC, NCIC check, LNSP screening).

(b) Results of background checks that do not uncover any adverse information will be forwarded to the sponsoring organization.

(c) Results of background checks that uncover adverse information will be forwarded to the responsible installation security office, and the sponsor will be notified of the adverse information. The area commander's adjudication board will coordinate with the sponsoring organization to determine whether the adverse information warrants denial of access privileges.

1. If the area commander recommends approval for local access, and the request includes installations outside the area commander's AOR, the request will be forwarded to the appropriate area commanders for adjudication. Adjudication packages must include the installation commander's approval memorandum, AEA Form 190-16A, the LNSP screening results, a GCC, and any supporting memorandums from the applicant and the applicant's supervisor.

2. If the area commander denies the applicant a pass based on the adverse results of a background check, the applicant must not be placed on an access roster.

(d) If an applicant is unable to obtain a background check, the IACO should review the situation and make a determination based on a risk assessment. IACOs can reduce their risks by using one or more of the following strategies:

1. Require non-HN resident applicants to provide their country's equivalent of the GCC and require this document to be translated into English and to be notarized.

2. More closely scrutinize access requirements and limit the number of installations to which access is authorized and the times at which it is authorized.

3. Deny visitor sponsor privileges to anyone who belongs to a category that allows these privileges but cannot provide the required background check information.

4. Limit the period of validity of the pass to have the expiration date coincide with the date on which the individual will have 12 months of residency in the HN and will qualify for the required background check. The pass will be limited to 1 year for applicants who do not reside in Germany.

(5) Residence and Work Permits. IACOs will follow applicable HN laws on acceptable residence documents and work permits. In Germany, for example, third-country citizens (non-EU nationals) are issued the electronic "*Aufenthaltstitel*" (glossary) as proof of legal residency; in Italy, third-country citizens (non-EU nationals) are issued a *permesso di soggiorno* (Italian permit to stay).

(6) Access Areas. Specific justification is required for an individual to gain access to an installation. The individual's sponsoring official will do the following:

(a) Ensure that the application indicates the minimum number of installations to which access is required by referring to the source documents supporting the requirement (for example, a contract performance work statement (PWS) listing specific names of installations).

(b) If an individual requires temporary access to another installation (for example, to attend training or a conference, to accept an unscheduled delivery), the sponsor may send an AEA Form 190-16A requesting temporary access to the appropriate IACO. The current pass will be updated electronically.

(c) If an individual requires recurring access to another area commander's installation, the sponsor must also request access from the IACO serving that installation. AEA Form 190-16A will be sent by email, and the current pass will be updated electronically. The individual does not have to visit the office or be issued another pass. Contact information for IACOs is listed on the IACS SharePoint site at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*.

(7) Authorized Days and Times. An individual's sponsoring official must review the installation access requirement and limit access to the minimum days, times, and locations required (for example, Clay Kaserne on Mondays from 08:00 to 09:00; Hainerberg on Mondays from 10:00 to 11:00; and Sembach on Tuesdays from 10:00 to 12:00). Since access is validated electronically and not printed on the card, it is possible to limit access to what is specifically needed.

(8) Visitor Sponsor Privileges. Applications must provide sufficient justification that clearly explains why an installation pass holder requires visitor sponsor privileges. Only area commanders or their designees are authorized to review and approve requests for visitor sponsor privileges.

(9) FPCON Restrictions. FPCON restrictions are based on an individual's category and function (nonessential, essential, "first or emergency responder" (glossary)). The IACS prohibits access beyond the FPCON associated with a pass category (paras 16 through 28). For access during FPCON Charlie, the sponsor must state the "essential functions" (glossary) that must be performed. For access during FPCON Delta, the sponsor must state the first or emergency responder functions (for example, fire or medical functions; critical mechanical, electrical, or water functions) or the duties the individual is required to perform in times of crises or war.

b. Processing an Application.

(1) Sponsoring officials will complete AEA Form 190-16A in English using U.S. standard measurements (app B) and will digitally sign the form to request a pass or to register a blue-stripe CAC. Sponsors who do not have a CAC (for example, members of a U.S. consulate human resources staff) may manually sign AEA Form 190-16A.

(2) Applicants will provide the sponsoring official the following documentation with the application:

(a) One of the documents in 1 through 3 below. Applicants must bring the original document with them to the registration office.

1. A copy of their passport.

2. A copy of their national ID card issued by the country of citizenship (for example, the *Personalausweis* in Germany, the *Identiteitskaart* or *carte d'identité* in Belgium, the *carta d'identità* in Italy).

3. Their U.S. Department of State or NATO ID; or their HN military, national police, and customs ID (for example, *Dienstausweis* in Germany). These documents may not be copied. Sponsoring officials may only view these documents during the registration process.

(b) The agreement justifying the need for installation access and confirming the expiration date (for example, "in loco parentis" (glossary) memorandum, AE Form 600-700A, contract or contract summary).

(c) GCC.

(d) If required, verification that the applicant has valid residence and work permits.

(3) When an application is complete, the sponsoring official will send it by email to the responsible IACO. The email message must be sent encrypted or through the DOD Secure Access File Exchange (SAFE) site (*https://safe.apps.mil*).

(4) The IACO will verify that the email message was submitted by an authorized sponsoring official by checking DD Forms 577 provided by the sponsoring organization.

(5) The IACO will verify that the HN background check (for example, the LNSP screening), if applicable, was initiated or completed as required per the category of pass requested.

(6) The IACO will review the application and supporting documents and will reject any application that is not complete. The IACO will also obtain clarification for applications with insufficient justification.

(7) The IACO will notify the sponsor when the application is approved.

(8) The sponsor will notify the applicant when the application is approved and will provide the applicant the required details for visiting the IACO and completing the application process. Applicants must bring their original passport or ID card to the IACO to validate their identity. For first-time issue of a pass, sponsors will either escort applicants to the IACO, place them on an access roster (AEA Form 190-16F), or coordinate initial access as specified through local procedures.

(9) Before the IACO issues a pass to an applicant, the applicant must sign AEA Form 190-16E and AEA Form 190-16K. The registrar will ensure that the applicant reads and understands the contents of the forms before signing them. A new AEA Form 190-16K must be signed each time a pass is issued or renewed.

(10) If an applicant does not speak, read, or understand English or the HN language, the sponsor is responsible for having someone available during the application process to provide translation services and to ensure that the applicant understands his or her responsibilities and the contents of the documents to be signed.

(11) The registrar will electronically file the completed application packet in accordance with the component's records information management system.

13. PROCEDURES FOR RENEWING A PASS

a. To renew a pass, sponsoring officials will submit a new application (AEA Form 190-16A). Requests may be processed as early as 90 days before the expiration date of the current pass. IACOs may issue a pass up to 90 days after the expiration date if an individual is unavailable to renew the pass earlier (for example, because of illness, injury, temporary duty travel).

b. If required by the category, a new GCC or U.S. Security Check is required if it is older than 12 months. In addition, a new AEA Form 190-16K must be signed when a pass is renewed.

c. In Germany, unless extraordinary circumstances exist (for example, documented evidence of criminal behavior), or required based on the individual's job description (for example, armed guard driver), a new LNSP screening is not authorized per AEA Regulation 604-1. Sponsoring officials will use the verification from the original LNSP screening.

d. To maintain continuity of records, passes will be renewed at the IACO that issued the initial pass, whenever possible.

e. Before issuing a new pass, IACOs will ensure that applicants turn in their expiring or expired pass, provide DA Form 4137 (or component equivalent) showing that access control personnel confiscated the pass, or provide a military police report showing that the card was lost or stolen.

f. Individuals in the Foreign Government Civilian/Local National Employee category (para 19) who transfer from one organization of the U.S. Forces to another without a break in service retain their status and are not required to provide a new GCC.

14. PROCEDURES FOR REPLACING A LOST OR STOLEN PASS

If a pass is lost or stolen, the pass holder must immediately report the loss or theft to the local MP and the servicing IACO. The pass will be flagged as lost or stolen. The sponsoring organization must submit a new application to the same IACO that issued the original pass.

15. UNSERVICEABLE PASSES
An unserviceable pass may be exchanged at the servicing IACO without action by the sponsoring organization. If the pass was confiscated by an MP official or access control personnel, the receipt (DA Form 4137 or component equivalent) will be used to obtain a new pass. The expiration date on the replacement pass will be the same as on the original pass.

SECTION V
INSTALLATION PASS CATEGORIES AND REQUIREMENTS

Individuals who do not qualify for a DOD ID card may be issued an installation pass from one of the categories defined in paragraphs 16 through 28.

16. CONVEYANCE

a. Definition: A broad category for individuals requiring recurring access to U.S. Forces installations for official business or based on an official relationship with the U.S. Government. The examples below are not all-inclusive. Sponsoring organizations will not use this category when an applicant meets the definition of another, more restrictive category. Examples are as follows:

(1) Official guests whose visits are based on a co-use agreement with the U.S. Government (for example, official visits from other U.S. Federal agencies).

(2) Gold Star and next of kin (NOK) survivor Family members who have a survivor access card. Survivor Family members will contact the installation Survivor Outreach Services or Army Community Service office to verify eligibility and coordinate their visit to the IACO.

(3) U.S. citizens or permanent resident interns participating in exchange programs.

(4) Individuals with member-of-household status. These guests are required to present their AEA Form 600-700A for verification.

(5) New U.S. Government civilian hires who cannot immediately receive a CAC.

(6) Individuals approved on a Family Care Plan (DA Form 5305 or DAF Form 357).

(7) Members of military community youth ministries (including Club Beyond), and Cadence International and its youth ministries arm, Malachi Ministries.

(8) Department of State and U.S. embassy personnel. This includes individuals assigned to or on duty with the Department of State, with a U.S. embassy in the USEUCOM AOR, or at U.S. diplomatic or consular posts according to AEA Reg 600-700.

(a) This example is a special category. The United States Mission in the country in which an individual is stationed will sponsor this category and send DD Forms 577 designating sponsoring officials by email to the OPM at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil*.

(b) Individuals in this category may obtain their installation pass at any IACO. Since these individuals are located throughout Europe, their first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the IACO. Background checks and residence and work permits are not required, and no restrictions exist; full access is authorized.

b. Expiration:

(1) Valid for 1 year or until the expiration date of the supporting document that was used to obtain the installation pass (for example, visa, passport), whichever is earlier.

(2) Exceptions:

(a) Gold Star and NOK survivor Family member passes are valid for up to 3 years or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earlier.

(b) Department of State and U.S. embassy personnel passes are valid for the length of the individual's tour (not to exceed 3 years) or until the expiration date of the supporting document (for example, passport, AE Form 600-700A) that was used to obtain the installation pass, whichever is earlier.

c. Sponsor: The organization requesting installation access will perform sponsor responsibilities.

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The LNSP screening must be initiated before the pass is issued.

(4) Exceptions to the Requirement for Background Checks:

(a) Department of State and U.S. embassy personnel and individuals with member-of-household status.

(b) Gold Star and NOK survivor Family members who have been vetted during the past 3 years and have been issued a survivor access card by another CONUS installation (for example, an Automated Installation Entry card).

(c) Because of the broad nature of this category, the responsible area commander, or the commander's designee, may grant ETPs on a case-by-case basis.

e. Residence and Work Permits: A residence permit may be required for individuals in this category depending on the individual circumstances.

f. Authorized Access: Limited to the minimum number of installations to which access is required based on the individual's official relationship with the U.S. Government.

g. Authorized Days and Times: Limited to the minimum based on the individual's official relationship with the U.S. Government, with the exception of the following individuals, who are authorized 24/7 access:

(1) Department of State and U.S. embassy personnel.

(2) Gold Star and NOK survivor Family members.

(3) Individuals with member-of-household status.

(4) Members of military community youth ministries (including Club Beyond), and Cadence International and its youth ministries arm, Malachi Ministries.

h. Visitor Sponsor Privileges: The following individuals are authorized visitor sponsor privileges:

(1) Department of State and U.S. embassy personnel.

(2) Gold Star and NOK survivor Family members.

(3) Individuals with member-of-household status.

(4) Military community youth ministries (including Club Beyond), and Cadence International and its youth ministries arm, Malachi Ministries.

(5) Individuals approved by the area commander or the commander's designee.

i. FPCON Restrictions:

(1) Nonessential personnel: Bravo.

(2) "Essential personnel" (glossary): Charlie.

(3) Essential personnel who are also first or emergency responders, personnel required to perform duties in times of crises or war, and individuals with member-of-household status: Delta.

17. FACILITY USE/VENDOR

a. Definition: A vendor who provides merchandise or services not associated with a Government contract. An example would be an individual who is authorized to offer insurance, real estate, or securities for sale, or merchandise (goods) or services (for example, food services such as selling ice cream or chicken from a truck) on U.S. Forces installations, but whose services are not associated with a Government contract.

b. Expiration: Valid for 1 year, until the expiration date of the supporting document (for example, visa, passport), or until the expiration date of the vendor's permit, whichever is earlier.

c. Sponsor: The IACO for the installation where the vendor conducts business. When access to more than one installation is required, the applicant must be sponsored by the Army and Air Force Exchange Service; the Defense Commissary Agency, Europe; or IMCOM-E. This sponsoring authority may not be delegated to subordinate organizations.

d. Background Checks: All background checks must be completed before a pass is issued.

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The screening must be completed and returned with no entries before a pass may be issued.

e. Residence and Work Permits: May be required for non-EEA citizens.

f. Authorized Access: Limited to the installations (listed by name) on which the vendor is authorized to provide goods or services.

g. Authorized Days and Times: Limited to the days and times the vendor is authorized to provide goods and services.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

18. FOREIGN CIVILIAN VISITOR

a. Definition: A foreign civilian who has been invited by the U.S. Government or who requires extended installation access for official purposes (for example, a VIP, a dignitary, a foreign civilian student assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany).

b. Expiration: Valid for 1 year, until the expiration date of the supporting document, or for the length of a student's tour, whichever is earlier.

c. Sponsor: The requesting organization sponsoring the individual (for example, the Marshall Center).

d. Background Checks: Determined by the area commander or the commander's designee based on the purpose of the visit.

e. Residence and Work Permits: Not required.

f. Authorized Access: Limited to the installations required for the official visit.

g. Authorized Days and Times: Limited to the minimum based on the purpose of the visit.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restrictions:

(1) Default: Bravo.

(2) Marshall Center Students: Delta.

19. FOREIGN GOVERNMENT CIVILIAN/LOCAL NATIONAL EMPLOYEE

a. Definition. A member of the HN government who requires recurring access for official business or based on an official relationship; a local city official (for example, mayor, fire chief, police chief, forestry official) or employee of the HN government; or a citizen or resident of the HN who is employed by or performing work for the DOD or State Department under an employment contract. The provisions in this paragraph also apply to individuals employed by the HN military working on U.S.-controlled installations and to HN interns.

b. Expiration: Valid for up to 3 years or until the expiration date of the supporting document (for example, passport), whichever is earlier.

c. Sponsor: The organization with the official relationship to the HN government official or the LN employee's supervisor.

d. Background Checks:

(1) GCC: Required before a pass may be issued. A GCC is not required for renewal.

(2) U.S. Security Check: Required for U.S. citizens before a pass may be issued.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The LNSP screening must be processing before a pass may be issued.

(4) Exceptions: The following categories of individuals are already vetted and do not require additional background checks:

(a) LN employees hired by a U.S. consulate.

(b) LN employees with a current U.S. or NATO Secret or higher clearance.

(c) Individuals with a DOD CAC.

(d) HN government officials providing a government ID card (for example, *Dienstausweis* in Germany).

e. Residence and Work Permits: Required for employees who are not citizens of an EEA member country. The USAREUR-AF IACS SharePoint site at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS* provides current guidance.

NOTE: In Germany, separate work permits are no longer issued. For individuals who are not citizens of an EEA member country, authorization to work must be included in and explicitly indicated on the *Aufenthaltstitel*.

f. Authorized Access: Limited to the minimum number of installations required to perform assigned duties.

g. Authorized Days and Times: Limited to the minimum required to perform assigned duties, or, for LN employees, based on the work schedule as determined by the sponsor.

h. Visitor Sponsor Privileges: For official use only, as justified by the sponsoring organization. Visitor sponsor privileges, if authorized, may not be granted until the HN background check is complete with no entries. Visitor sponsor privileges are not authorized during FPCONs Charlie and Delta.

i. FPCON Restrictions:

(1) Nonessential personnel: Bravo.

(2) Essential personnel: Charlie.

(3) Essential personnel who are also first or emergency responders, and personnel required to perform duties in times of crises or war: Delta.

20. FOREIGN GOVERNMENT CONTRACTOR

a. Definition: An individual without NATO SOFA status who lives in the EU or in a NATO member country and is contracted to work for the DOD in Europe. Contractors without an existing contract must be signed in as a guest or placed on an access roster.

b. Expiration: Valid for 3 years or until the expiration date of the supporting document (for example, visa, passport), whichever is earlier.

c. Sponsors:

(1) Individuals appointed in writing as CORs, ACORs, or SCORs. CORs, ACORs, or SCORs who are not available to perform the sponsor function (for example, if based in CONUS) may appoint in writing an individual assigned to the USEUCOM AOR as their representative for sponsoring installation access.

(2) Individuals appointed in writing as sponsors for contractors by an OPM-approved agency or organization (for example, the 266th Finance Support Center sponsors Community Bank contractors).

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The LNSP screening must be initiated before a pass is issued.

e. Residence and Work Permits: Required for individuals who are not citizens of an EEA member country. The USAREUR-AF IACS SharePoint site at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS* provides current guidance.

NOTE: In Germany, separate work permits are no longer issued. For individuals who are not citizens of an EEA member country, authorization to work must be included in and explicitly indicated on the *Aufenthaltstitel*.

f. Authorized Access: Limited to the minimum number of installations required for a contractor to perform duties according to the contract PWS or other contract documentation.

g. Authorized Days and Times: As specified in the PWS or other contract documentation.

h. Visitor Sponsor Privileges: Area commanders or their designees may approve visitor sponsor privileges for official use based on the justification provided on AEA Form 190-16A, as supported by the PWS.

(1) Only third-party contractors and vendors who support the sponsor's contract may be sponsored for an escorted visitor paper pass.

(2) Visitor sponsor privileges for installation pass holders are not authorized during FPCONs Charlie and Delta.

i. FPCON Restrictions:

(1) Nonessential personnel: Bravo.

(2) Essential personnel: Charlie.

(3) Essential personnel who are also first or emergency responders, and personnel required to perform duties in times of crises or war: Delta.

21. FOREIGN MILITARY/FOREIGN MILITARY DEPENDENT

a. Definition:

(1) A NATO military member, civilian employee, and their dependent Family members (up to age 21). This category is designed for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military) who meet the requirements in AEA Reg 600-700 for NATO personnel assigned to an international military headquarters in Germany, and for foreign liaison officers from NATO member states assigned to a U.S. military headquarters (for example, USEUCOM, USAREUR-AF, USAFE/AFAFRICA).

(2) A member of the armed forces of a foreign nation and the member's accompanying Family members (children up to the age of 21) who are stationed on a U.S. Forces-controlled installation.

(3) A foreign military student assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany.

b. Expiration: Valid for up to 3 years, for the length of the non-U.S. military member's tour or class dates, or until the expiration date of the supporting document (for example, a military ID card), whichever is earlier.

c. Sponsor: The responsible U.S. liaison organization (for example, the Marshall Center for its students).

d. Background Checks: Not required.

e. Residence and Work Permits: Not required.

f. Authorized Access: NATO members are limited to the country of their assignment. HN military members are limited to the minimum number of installations required to perform their assigned duties. Students are limited to the location of instruction and dormitories.

g. Authorized Days and Times: As specified by the sponsor.

h. Visitor Sponsor Privileges: Authorized.

i. FPCON Restrictions: None.

22. LONG-TERM VISITOR

a. Definition: An immediate Family member of the "requester" (glossary), age 16 or older. For the purpose of this publication, immediate Family members include the requester's sons, daughters, parents, brothers, sisters, mother-in-law, father-in-law, brothers-in-law, sisters-in-law, grandparents, and grandparents-in-law.

b. Expiration: Valid for the duration of the visit, up to 90 days for Family members residing outside the EEA, and up to 1 year for Family members who are legal residents of the EEA. The duration is subject to the expiration date of the supporting document (for example, visa, passport).

c. Sponsor: A DOD ID cardholder who is 18 years or older and residing on a military installation or in leased Government housing. If the requester resides off a military installation or leased Government housing, the area commander or the commander's designee may approve a pass based on the extenuating circumstances presented by the requester. Sponsor training is not required.

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

NOTE: Minors under the age of 18 do not require background checks.

e. Residence Permit: Required for passes of more than 90 days for non-EEA citizens.

f. Authorized Access: Limited to installations where the requester resides. Requesters visiting another installation with their Family members may request access through the installation IACO.

g. Authorized Days and Times: As specified by the sponsor.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

23. PERSONAL DELIVERY (RECURRING DELIVERIES OR SIMILAR SERVICES NOT ASSOCIATED WITH A GOVERNMENT CONTRACT)

a. Definition: Individuals who need recurring access to U.S. Forces installations to make deliveries or to perform similar services related to their employment (for example, pizza delivery personnel, taxi drivers).

b. Expiration: Valid up to 1 year or until the expiration date of the supporting document (for example, passport), whichever is earlier.

c. Sponsor: The U.S. Forces organization for which deliveries are made or services are performed, or the responsible area commander or IACO.

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The screening must be completed and returned with no entries before a pass may be issued.

e. Residence and Work Permits: Required for individuals who are not citizens of an EEA member country. The USAREUR-AF IACS SharePoint site at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS* provides current guidance.

f. Authorized Access: Limited to installations needed to provide services.

g. Authorized Days and Times: Limited to the days and times required to provide services.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

24. PERSONAL SERVICES

a. Definition: An individual hired and on contract by a requester to perform a service (for example, a nanny, a housecleaner).

b. Expiration: Valid for 1 year, until the expiration date of the supporting document (for example, visa, passport), or through the length of service, whichever is earlier.

c. Sponsor: The base IACO where the requester resides. The IACO is required to review the contract for services as part of the application process.

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The screening must be completed and returned with no entries before a pass may be issued.

e. Residence and Work Permits: May be required for non-EEA citizens.

f. Authorized Access: Limited to the installation where the requester resides.

g. Authorized Days and Times: Limited to the time required by the contract.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

25. PRIVATIZED HOUSING

a. Definition: Individuals and their dependents who physically reside in their personal residence, or individuals who require access to their private land on an installation controlled by the U.S. Forces (for example, H tenants residing on Smith Barracks, USAG Rheinland-Pfalz; farmers at USAG Benelux, Chièvres Air Base).

b. Expiration: Valid up to 3 years or until the expiration date of the supporting documents (for example, passport), whichever is earlier.

c. Sponsor: The responsible organization assigned as the residence or land owner's point of contact.

d. Background Checks: Not required.

e. Residence and Work Permits: Not required.

f. Authorized Access: The installation where the personal residence or private land is physically located.

g. Authorized Days and Times: 24/7.

h. Visitor Sponsor Privileges: Authorized to sponsor a pass in the following categories for the installation where individuals physically reside in their personal residence:

(1) Long-Term Visitor (para 22).

(2) Personal Delivery (para 23).

(3) Personal Services (para 24).

i. FPCON Restriction: Delta.

26. U.S. GOVERNMENT CONTRACTOR

a. Definition: A U.S. citizen without NATO SOFA status who is working for a U.S. company based in the United States and is contracted to work temporarily for the DOD in Europe.

b. Expiration: Valid for the length of the visit or up to 90 days, whichever is shorter; or valid up to 1 year if the contractor will be making multiple short trips throughout the year not to exceed a total of 90 days. For visits to Germany, a "BACO-90" (see note below) form is required before arriving in Germany. AEA Reg 715-9 provides procedures for the BACO-90 application process. For other countries, the sponsor is responsible for ensuring that all required country documents are completed before the contractor arrives in theater.

NOTE: "BACO-90" is a shorthand term referring to the process of obtaining "Confirmation of the Exemption from the Requirement to Obtain a German Work Permit." Additional information can be found on the website of the DOD Contractor Personnel Office (DOCPER), Civilian Personnel Division, Office of the Deputy Chief of Staff, G1, HQ USAREUR-AF (*https://www.europeafrica.army.mil/contractor/*).

c. Sponsors: Individuals appointed in writing as CORs, ACORs, or SCORs. CORs, ACORs, or SCORs who are not available to perform the sponsor function (for example, if based in CONUS) may appoint in writing an individual assigned to the USEUCOM AOR as their representative for sponsoring installation access. In Germany and Italy, sponsors must ensure compliance with DOCPER policy (AEA Reg 715-9).

d. Background Checks: A U.S. security check is required.

e. Residence and Work Permits: Depending on the HN and applicable agreements, residence and work permits may be required. AEA Reg 715-9 and the DOCPER website at *https://www.europeafrica.army.mil/contractor/* provide further guidance.

f. Authorized Access: Limited to the minimum number of installations required for a contractor to perform duties according to the contract PWS or other contract documentation.

g. Authorized Days and Times: As specified in the PWS or other contract documentation.

h. Visitor Sponsor Privileges:

(1) Not authorized, except as stated in (2) below.

(2) Area commanders or their designees may approve visitor sponsor privileges for official use based on the justification provided on AEA Form 190-16A, as supported by the PWS. Only third-party contractors and vendors who support the contract may be sponsored for an escorted visitor paper pass.

i. FPCON Restrictions:

(1) Nonessential personnel: Bravo.

(2) Essential personnel: Charlie.

27. VOLUNTEER

a. Definition: An individual identified as a volunteer who requires recurring and unescorted access. Examples include, but are not limited to, volunteers supporting chapel programs, United Service Organizations, Fisher House, Red Cross, or Family and morale, welfare, and recreation facilities. Sponsors will submit a justification for access to the servicing IACO, which will review the access requirements.

b. Expiration: Valid for 1 year or until the expiration date of the supporting document (for example, visa, passport), whichever is earlier.

c. Sponsor: The organization requesting access for the volunteer.

d. Background Checks:

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The screening must be completed and returned with no entries before a pass is issued.

NOTE: In Germany, if there is a 90-day or longer delay in receiving LNSP results, or if a pass is required immediately due to extenuating circumstances, the area commander or the commander's designee may approve the pass before receiving the completed LNSP screening.

e. Residence and Work Permits: Required for passes of more than 90 days for non-EEA residents.

f. Authorized Access: Limited to installations where the individual is providing volunteer services.

g. Authorized Days and Times: Limited to the days and times required to perform volunteer services.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

28. OTHER

a. Definition: Individuals who require recurring and unescorted access, but who do not meet the definition of any other person category. IACOs will review the access requirements for each applicant and evaluate the extenuating circumstances based on the area commander's policy. The following are examples for this category: a DOD retired civilian or a retired LN employee with a retirement SF 50; a member of an approved private organization (PO) who has no reason to enter U.S. Forces installations other than to participate in PO functions; a spouse or dependent who transports an installation pass holder who has a permanent physical handicap or is temporarily disabled (for example, broken leg, recent surgery); parents or guardians of DOD dependents.

b. Expiration: Valid up to 1 year or until the expiration date of the supporting document (for example, passport), whichever is earlier.

c. Sponsor: An individual who has knowledge of the access requirement and accepts the responsibility. Examples include an area commander who authorizes a DOD retired civilian or a retired LN employee an installation pass, or an LN supervisor whose employee is temporarily disabled with a broken leg and requests a pass for the spouse to drive the employee to and from work.

d. Background Checks: All required background checks listed below must be completed before issuing a pass. In Germany, if there is a 90-day or longer delay in receiving LNSP results, or if a pass is required immediately due to extenuating circumstances, the area commander or the commander's designee may approve the pass before receiving the completed LNSP screening.

(1) GCC: Required for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status.

(2) U.S. Security Check: Required for U.S. citizens.

(3) HN Background Check: Required, if available, for non-U.S. citizens and for U.S. citizens who have lived in the HN for more than 12 consecutive months without NATO SOFA status. In Germany, this is the LNSP screening. The LNSP must be completed and returned with no entries before a pass may be issued, except as stated in subparagraph d above.

e. Residence and Work Permits: Required for individuals who are not citizens of an EEA member country. The USAREUR-AF IACS SharePoint site at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS* provides current guidance.

f. Authorized Access: Limited to the minimum number of installations required.

g. Authorized Days and Times: Limited to the minimum required.

h. Visitor Sponsor Privileges: Not authorized.

i. FPCON Restriction: Bravo.

SECTION VI
ACCESS PROCEDURES

29. ESCORTED VISITOR PAPER PASS

The escorted visitor paper pass (fig 3) provides short-term access for 1 to 30 days (maximum), unless further restricted by local policy. It is used when an access roster and an installation pass are impractical or not authorized.

Figure 3. Sample Escorted Visitor Paper Pass

a. Visitor Sponsor Privileges.

(1) Personnel with sign-in privileges who are 18 years old or older may escort visitors. If this privilege has been revoked, the revocation will be documented in the IACS. ACP guards will be notified automatically by IACS if visitor sponsor privileges have been revoked.

(2) Visitor sponsor privileges are documented on the front of all installation passes, with any qualifications (for example, “contractors and vendors only”) listed in the remarks block on the back.

b. Restrictions.

(1) Visitor sponsors are limited to sponsoring four individuals and their vehicles at any one time. Area commanders or their designees may authorize an ETP to allow sponsoring up to 10 individuals and their vehicles.

(2) Individuals who require recurring access cannot use the visitor pass to circumvent the installation pass application process or access roster requirements.

(3) When visitor sponsor privileges are abused or violate local policy, area commanders may revoke them.

(4) No fingerprints will be taken when issuing the visitor pass. This applies to both U.S. and non-U.S. citizens.

c. Identification. Individuals requesting a visitor paper pass must show the ACP guard their valid passport, national ID (for example, the *Personalausweis* in Germany, the *Identiteitskaart* or *carte d'identité* in Belgium, the *carta d'identità* in Italy), NATO ID, non-U.S. military ID, or police or customs ID (for example, *Dienstausweis* in Germany). Guards will use the document scanner to upload the information into IACS and will conduct a visual comparison to ensure that the ID belongs to the requester. Visitors are required to show the guard the ID that was used to generate the visitor pass when the guard scans the pass.

d. Sponsor Responsibilities. Sponsors will ensure that their visitors are physically escorted at all times. Sponsors who cannot escort their visitors themselves may transfer that responsibility to another authorized sponsor who will print and sign their name and provide a telephone number on the back of the paper pass. Sponsors who do not physically escort their visitors and fail to correctly transfer sponsorship to another sponsor will lose their visitor sponsor privileges for 30 days for the first offense, for 120 days for the second offense, and for 1 year for the third offense. Area commanders may provide additional restrictions and limitations.

e. Technical Difficulties. If a network connection is unavailable or the printer is inoperable at the visitor gate, guards will use manual procedures as approved by local policy.

f. AEA Form 190-16E, Data Protection Statement and Consent to the Collection, Storage, and Use of Personal Data. Individuals who are not citizens or permanent residents of the United States are required to read AEA Form 190-16E and sign the form or visitor log book before receiving their escorted visitor paper pass.

g. Language Assistance. If applicants do not speak, read, or understand English or the HN language, sponsors are responsible for ensuring that the applicants understand their responsibilities and the contents of the documents to be signed.

30. ACCESS ROSTERS

a. Access rosters provide short-term unescorted access. They must be coordinated in advance using AEA Form 190-16F and must be approved by the area commander or the commander's designee.

b. Access roster requests must be submitted no later than 3 workdays before the desired effective date of the roster. If approved, they will be forwarded to the ACP before the effective date.

c. Access rosters are limited to 30 days, are site-specific, and are used for events that are nonrecurring and not regularly scheduled. The following are examples of when an access roster is appropriate: a unit or personal event such as a birthday party or a change of command; inprocessing of new employees; meetings that include nonaffiliated or HN personnel; contractors performing short-term, site-specific work.

d. Access rosters are temporary and will not be used to circumvent the IACS pass process. Individuals may not be put on an access roster for more than 30 days. If more time is required, the sponsor will request an installation pass through the IACO.

e. U.S. citizens are required to have a NCIC III background check. Non-U.S. contractors or vendors must submit a current GCC that is less than 12 months old.

f. Individuals with an adverse background check (NCIC check, GCC, or LNSP screening) that has not been adjudicated will not be placed on an access roster.

g. Area commanders or their designees may provide ETPs to background checks.

h. Approved access rosters are forwarded to the ACP. ACP guards will issue an unescorted visitor paper pass to the individuals listed on AEA Form 190-16F and will enter "Unescorted" in the remarks section.

i. The following policies apply to access rosters:

(1) Personnel with visitor sign-in privileges who are 18 years old or older may sign requests for access rosters. Area commanders or their designees may grant exceptions or further restrict authorized sponsors. IACOs will confirm that requesters have visitor sign-in privileges and will review local policy to ensure that requesters are authorized to sign access roster requests.

(2) Requests for access rosters must be sent from official email accounts (for example, accounts ending in .aafes.com, .eu.dodea.edu, .gov, .mil, .nato). All requests must be sent by encrypted email or through the DOD SAFE site (*https://safe.apps.mil/*). IACO officials will confirm receipt.

31. EMERGENCY VEHICLE ACCESS

a. Access During an Emergency.

(1) During a coordinated emergency response, when the MP desk has called for assistance, clearly marked emergency vehicles (HN and U.S.) with sirens on or lights flashing will not be stopped for ID checks. The MP desk will notify the appropriate ACP to allow for unimpeded access.

(2) In situations where the HN emergency response has not been coordinated through the MP desk, the gate guard at the ACP will require emergency vehicles to come to a stop to allow guards an opportunity to quickly identify the driver and their purpose, and will notify the MP desk.

(3) Ambulance service is provided by HN hospitals. Installation physical security managers should include a description of HN ambulances in their local standard operating procedures (SOPs).

b. HN Police.

(1) When on routine patrol or investigative duty, HN police are required to present their official ID when entering U.S. installations, even if they are in marked police vehicles and wearing HN police uniforms. Installation physical security offices should include a description of HN police IDs in local SOPs. If there is any reason to doubt the validity of an ID or the reason for entering an installation, the guard will call the MP desk.

(2) HN police who work on an installation with U.S. Forces police and do not have a blue-stripe CAC may be issued an installation pass using the Foreign Government Civilian/Local National Employee category (para 19) to access the installation.

c. Other HN Service Providers. Installation physical security managers should develop alternate access control procedures for other HN service providers who respond to emergencies that are not life threatening (for example, providers of water, electric, or heating services). In these situations, unimpeded access should not be granted. Installation physical security managers should develop memorandums of agreement that require these service providers to notify the installation ahead of time when access is required.

32. SPECIAL VEHICLE ACCESS

a. Protective Services Vehicles.

(1) Protective services heavy armored vehicles (HAVs) and security escort vehicles (SEVs) do not have blanket authority to enter closed installations without the driver presenting proper credentials.

(2) ACP guards will not stop HAVs or SEVs that have been granted unimpeded access through coordination with the responsible local physical security personnel. ACP guards will be provided descriptions and license plate numbers of expected vehicles and the expected time of the visit. Once recognized by the guard, the vehicles will be waved through the gate without delay.

(3) In cases where prior coordination was not accomplished, only HAV drivers must present their DOD ID card (no dispatch, license, or other documents). Other occupants in HAVs will not be asked to provide an ID. Exceptions to this policy must be approved by the area commander.

(4) Guards will request that only the driver's window be opened to receive the driver's ID card. Guards will not look inside the vehicle, request the occupants to exit the vehicle, or try to search the vehicle.

(5) If an SEV is present, only the ID card of the HAV driver of the first (lead) vehicle will be checked. The lead HAV driver will inform the guards that the next vehicle is an SEV. The objective is to get these vehicles through the gate as quickly as possible without bypassing security procedures.

b. Arms Control Treaty Vehicles.

(1) U.S. forces in Europe are subject to inspections primarily under the Treaty on Conventional Armed Forces in Europe and the Vienna Document 2011. A component treaty compliance officer will notify the area commander of inspections and will coordinate access for teams conducting compliance inspections under these and other treaties. Inspection teams will arrive at U.S. installations under escort in vehicles provided by the HN.

(2) HN security personnel will search vehicles used to transport inspection teams before they arrive at an installation. Inspectors and the property under their control will be screened and cleared during "point of entry" procedures as specified under the applicable treaty. Inspectors are granted diplomatic privileges and immunities during inspections and, consequently, may not be searched again by gate guards, military LE, or security personnel.

(3) When a treaty inspection or exercise is conducted, the gate guard will follow the instructions of the area commander and the treaty compliance officer to allow access for treaty vehicles.

c. Trusted Traveler.

(1) During FPCON Bravo, area commanders may authorize "Trusted Traveler (TT)" (glossary) access for military shuttlebuses transiting between IACS-controlled installations. The ACP guard will scan the driver's DOD ID card or installation pass after verifying with the driver that no stops were made in transit between U.S.-controlled installations.

(2) When vehicles queuing at the ACP create unnecessary risk, MP or physical security officers may authorize TT access, scanning only one DOD ID card or pass per vehicle temporarily until the dangerous traffic situation is mitigated. The ACP guard will confirm that the driver of each vehicle will vouch for their passengers.

(3) Area commanders will suspend TT access during random AT measures.

(4) ACP guards may decide to scan all passengers on the bus or in a vehicle if an unusual situation exists.

(5) TT procedures must not be used during FPCONs Charlie and Delta.

33. COORDINATED ACCESS

a. Military Convoy Movements and Exercise Deployments (U.S., NATO, HN). If not already documented in local policy, area commanders or their designees may approve military convoy movements and exercise deployments. Military and exercise planners must coordinate these movements and account for all vehicles.

b. VIP Expedited Access. Area commanders or their designees may approve VIP expedited access. A protocol officer or a member of the requesting organization will coordinate the time and place of the visit and will be physically present at the ACP to verify the VIP's access and to escort the VIP during the visit on the installation.

c. Conferences. Conference planners will submit an access roster (AEA Form 190-16F) to coordinate the time and place of access for attendees. They may also specify which lane to use at the ACP, if applicable, and have a person physically present at the ACP to verify and account for conference attendees.

d. Ad Hoc Access. During times of crises or exceptional circumstances, area commanders or their designees may approve ad hoc access. Ad hoc access must be coordinated with the MP, who will provide support in physically escorting and monitoring visitors requiring access on and off the installation (for example, media crews approved to report on a location or to conduct an authorized interview).

e. Unmanned Entry Gates. Area commanders or their designees may approve local SOPs for authorized persons to access an installation (for example, farmers with tractors, individuals requiring access to rail heads). The unmanned gate is required to have the appropriate security measures to document and record when the gate is opened and closed.

34. ACP GUARDS

a. ACP guards (military, civilian, and contracted) will—

(1) Perform their duties in accordance with this publication and any special guard orders.

(2) Grant access only to individuals authorized access according to the policy and procedures in this publication. Access authorization must be verified for all individuals entering a U.S. Forces-controlled installation, including all passengers in a vehicle, except as prescribed in paragraph 32. Table 1 lists the appropriate actions based on responses from handheld personal digital assistance (PDA) scanners.

(3) Contact the MP desk when notified by an IACS alert or warning and follow the provided guidance and instructions.

(4) Follow the escorted visitor paper pass policy and procedures in paragraph 29, and the access roster policy and procedures in paragraph 29 for issuing unescorted visitor paper passes, and do the following:

(a) Ask individuals who are not U.S. citizens or permanent residents of the United States to read AEA Form 190-16E (in English, German, or Italian, whichever language is required) and to sign the form or visitor log book (manually or, if available, electronically). As a minimum, the visitor book will provide space for first and last names, date, and signature.

(b) Ask U.S. citizens and legal residents to read the Privacy Act Statement (app D) (no signature required).

(c) Use the passport reader to scan all ID documents that have a machine-readable zone (MRZ). If an ID document does not have an MRZ, the guard will manually and accurately enter the required information into the IACS.

(d) Take a photo of the visitor’s face.

(e) Ask the sponsor which installations the visitor will need to access and for how long the visitor paper pass should be valid (1 to 30 days, or as authorized by local policy).

(f) Enter the appropriate comments depending on whether the pass is an escorted visitor pass or an unescorted visitor pass issued based on an access roster.

(g) Complete the visitor pass application process.

(h) Print and have the visitor sign the visitor paper pass.

(i) When scanning the escorted visitor paper pass at the ACP, verify that the photo ID that was used to generate the escorted visitor pass matches the visitor.

b. All personnel conducting access control may confiscate DOD ID cards or installation passes. MPs will establish receipt procedures and will ensure that these documents are turned in to the servicing IACO or ID card issuing facility as appropriate.

c. When the IACS is unavailable (temporarily offline), guards will manually check access documents and ask for a second form of photo ID (for example, drivers license). If an individual does not have a second form of photo ID and is over the age of 16, the guard will contact the MP desk for additional guidance.

d. When the IACS is operational at an ACP, guards will scan 100 percent of DOD ID cards and installation passes unless emergency vehicles (para 31) or special vehicles (para 32) require access, or TT (para 32c) or coordinated access (para 33) procedures are active. TT procedures cannot be used during FPCONs Charlie and Delta.

e. When DOD ID cardholders or installation pass holders have forgotten their ID card or pass, guards will ask for a second form of ID, if available; conduct a manual lookup to positively identify the individual; and follow local procedures for authorizing access.

f. Minors under the age of 16 are not required to show a photo ID when accompanied by an adult (age 18 or older) with the required photo ID registered in the IACS. The adult (for example, a DOD ID cardholder in a minivan with children) will vouch for the children's identity and be responsible for their actions while on the installation.

g. When guards determine that a situation is not normal or routine, they are required to ask additional questions to clarify the purpose of the visit or the access requirement and, if there is any doubt, to contact the MP desk for support or instructions.

h. The PDA scanner provides three types of scanned returns: green = Access Granted, yellow = Access Warning, red = Access Denied (fig 4).

i. Guards will follow the required actions based on the scan responses in table 1. The "Required Action" column details actions to be taken for the various messages.

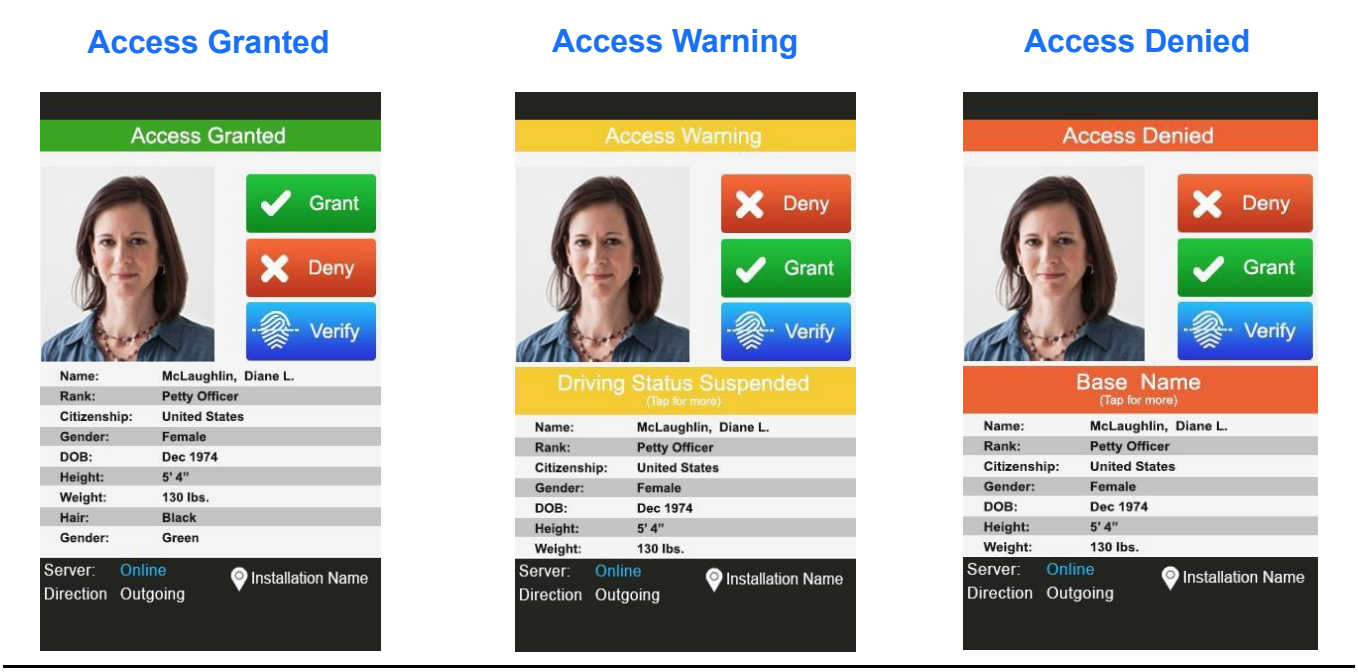

Figure 4. Sample PDA Responses

Table 1
PDA Scan Responses and Guard Actions

Condition Type	PDA Access Message	Required Action
Person Status	**RED - Armed and Dangerous**	**No access.** Raise barrier, contact MP desk for instructions.
	BARRED **- RED: barred at this base**	**No access.** Contact MP desk for instructions.
	- YELLOW: barred at other bases	**No access** unless approved by the area commander
	RED - Call Law Enforcement	**No access.** Contact MP desk for instructions.
	YELLOW - Driving Status Suspended	**Detain if the individual is driving the vehicle**, contact MP desk, and wait for MP patrol to arrive.
	RED - International Hold	**No access.** Contact MP desk for instructions.
	RED - Missing	
	RED - BOLO	
	RED - Unauthorized Absence	
	RED - Sex Offender Registration Alert	
	RED - Violent Person	
	RED - Site Suspension	
	RED - Wants Warrant Hold	
Expired Sponsor	**RED - Sponsor no longer valid**	**No access.** Contact MP desk for instructions.
ID Card Not Current	**RED – Expired ID card**	**No access.** Contact MP desk for instructions. If instructed, confiscate ID and issue DA Form 4137. Do not allow on post without escort.
Insufficient Permissions	**RED - Access not authorized at this time**	**No access during this time of day.** Do not allow on post without escort.
	RED - Access not authorized on this day	**No access on post during this day of the week.** Do not allow on post without escort.
	RED - Access denied at this FPCON level	**No access at this FPCON level.** Do not allow on post without escort.
	RED - Access denied at this HPCON level	**No access at this HPCON level.** Do not allow on post without escort or proper documents.
	RED - Access denied at this installation	**No access.** Do not allow on post without escort or proper documents.

j. “Encounter management” (glossary) is a process that begins at the ACP when the IACS alerts the guard with a yellow or red response, usually during a PDA scan. The ACP guard will follow the directions in table 1 and figure 5 and will contact the MP desk. When the IACS alerts the guard with a yellow or red response, the guard will—

(1) Advise the person to “stand by” and deny access.

(2) Read the message on the PDA and follow the instructions in table 1.

(3) Call the MP desk and wait for guidance.

(4) Not allow the persons in the vehicle to use a cell phone.

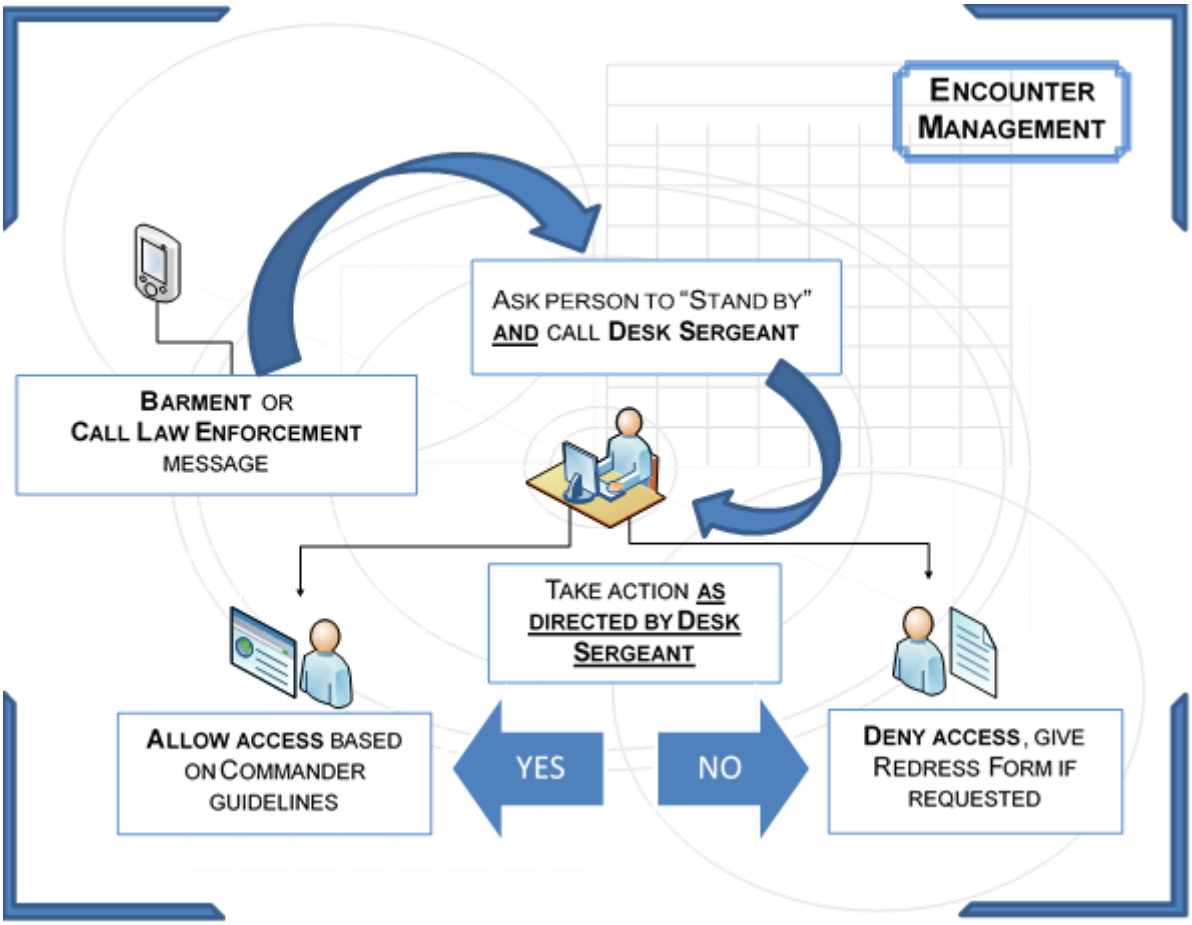

Figure 5. ACP Encounter Management Procedures

(5) Be prepared to raise the vehicle barrier.

(6) Provide the access denial redress form (AEA Form 190-16G) if the individual questions why access is denied.

APPENDIX A
REFERENCES

Army in Europe and Africa (AEA), Department of the Army (DA), and DOD publications and forms are available through the Army in Europe and Africa Publications (AEPUBS) website at *https://www.aepubs.eur.army.mil/* or *https://intranet.eur.army.mil/aepubs/*.
The glossary defines abbreviations used in this appendix.

SECTION I
PUBLICATIONS

United Nations Security Council Resolution 2178
Threats to International Peace and Security Caused by Terrorist Acts

Supplementary Agreement to the NATO Status of Forces Agreement

Treaty on Conventional Armed Forces in Europe

Vienna Document 2011

HSPD 6
Integration and Use of Screening Information to Protect Against Terrorism

EO 9397
Numbering System for Federal Accounts Relating to Individual Persons

Immigration and Nationality Act (PL 82-414)

Privacy Act of 1974 (PL 93-579)

Enhanced Border Security and Visa Reform Act of 2002 (PL 107-173)

8 USC 1101
Immigration and Nationality, Definitions

10 USC 136
Under Secretary of Defense for Personnel and Readiness

UCMJ Article 86
Absence Without Leave

DODI 1000.25
DOD Personnel Identity Protection (PIP) Program

DODI 5200.08
Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)

DODI 8500.01
Cybersecurity

DOD 5200.08-R
Physical Security Program

DOD 5400.11-R
Department of Defense Privacy Program

DOD Manual 5200.08, Volume 3
Physical Security Program: Access to DOD Installations

AD 2014-05
Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors

AR 15-6
Procedures for Administrative Investigations and Boards of Officers

AR 25-400-2
Army Records Management Program

AR 190-13
The Army Physical Security Program

AR 550-1
Processing Requests for Political Asylum and Temporary Refuge

AFI 33-322
Records Management and Information Governance Program

AFMAN 31-101V3
Installation Perimeter Access Control

CNIC-M 5530.2
Navy Installation Access Control

USEUCOM Antiterrorism OPORD 23-01

AEA Reg 25-400-2
Army in Europe Records Information Management

AEA Reg 27-9
Misconduct by Civilians

AEA Reg 27-10
Military Justice and Legal Operations

AEA Reg 190-1/CNE-CNA-C6F Inst 11240.6AB/USAFE-AFAFRICA Inst 31-202
Driver and Vehicle Requirements and the Installation Traffic Code for the U.S. Forces in Germany

AEA Reg 190-13
USAREUR Physical Security Program

AEA Reg 525-13
Antiterrorism

AEA Reg 525-50
Arms Control Compliance

AEA Reg 600-700
Identification Cards and Individual Logistic Support

AEA Reg 604-1
Local National Screening Program in Germany

AEA Reg 690-64
Standards of Conduct, Corrective Actions, Termination Process, and Grievances (Local National Employees in Germany)

AEA Reg 715-9
Contractor Personnel in Germany—Technical Expert, Troop Care, and Analytical Support Personnel

IACS Policy Memorandum #1
Identity Proofing
(available at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*)

IACS Policy Memorandum #2
EUCOM Transferring PII
(available at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*)

IACS Policy Memorandum #3
How to Take a Photo
(available at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*)

IACS Policy Memorandum #4
Encounter Management
(available at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*)

IACS Policy Memorandum #5
Changing the FPCON
(available at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*)

SECTION II
FORMS

SF 50
Notification of Personnel Action

SF 135
Records Transmittal and Receipt

DD Form 448
Military Interdepartmental Purchase Request

DD Form 577
Appointment/Termination Record – Authorized Signature

DD Form 2875
System Authorization Access Request (SAAR)

DA Form 3953
Purchase Request and Commitment

DA Form 4137
Evidence/Property Custody Document

DA Form 5305
Family Care Plan

DAF Form 357
Family Care Certification

AEA Form 190-16A
Application for Installation Access

AEA Form 190-16E
Data Protection Statement and Consent to the Collection, Storage, and Use of Personal Data for Non-U.S. Citizens and Permanent Residents / *Datenschutzerklärung und Einwilligung zur Erhebung, Speicherung und Verwendung personenbezogener Daten* / *Dichiarazione di Protezione dei Dati e Consenso al Trattamento dei Dati Personali per i Cittadini Non Statunitensi e Residenti Permanenti*

AEA Form 190-16F
Installation Access Roster Request

AEA Form 190-16G
Installation Access Redress Application

AEA Form 190-16K
Installation Pass Holder Acknowledgment of Responsibilities/*Anerkennung der Pflichten eines Ausweisinhabers/Responsabilità per i Dententori di Passi per Installazioni*

AEA Form 600-700A
Army in Europe Privilege and Identification Card

AEA Form 604-1A
Personnel Data Request (*Personaldaten Anfrage*)

AEA Form 604-1B
Security Questionnaire for a Simple Security Check

APPENDIX B
HEIGHT AND WEIGHT CONVERSION CHARTS

Weight Conversion Chart			Height Conversion Chart		
(2.2045 pounds = 1 kilogram)			(.39370 inches = 1 centimeter)		
Kilograms	**Pounds**		**Centimeters**	**Height in feet and inches**	**Inches**
35	77		122	4 feet 0 inches	48
37	82		124	4 feet 1 inches	49
39	86		127	4 feet 2 inches	50
41	90		130	4 feet 3 inches	51
43	95		132	4 feet 4 inches	52
45	99		135	4 feet 5 inches	53
47	104		137	4 feet 6 inches	54
49	108		140	4 feet 7 inches	55
51	112		142	4 feet 8 inches	56
53	117		145	4 feet 9 inches	57
55	121		147	4 feet 10 inches	58
57	126		150	4 feet 11 inches	59
59	130		152	5 feet 0 inches	60
61	134		155	5 feet 1 inches	61
63	139		157	5 feet 2 inches	62
65	143		160	5 feet 3 inches	63
67	148		163	5 feet 4 inches	64
69	152		165	5 feet 5 inches	65
71	157		168	5 feet 6 inches	66
73	161		170	5 feet 7 inches	67
75	165		173	5 feet 8 inches	68
77	170		175	5 feet 9 inches	69
79	174		178	5 feet 10 inches	70
81	179		180	5 feet 11 inches	71
83	183		183	6 feet 0 inches	72
85	187		185	6 feet 1 inches	73
87	192		188	6 feet 2 inches	74
89	196		191	6 feet 3 inches	75
91	201		193	6 feet 4 inches	76
93	205		196	6 feet 5 inches	77
95	209		198	6 feet 6 inches	78
97	214		201	6 feet 7 inches	79
99	218		203	6 feet 8 inches	80
101	223		206	6 feet 9 inches	81
103	227		208	6 feet 10 inches	82
105	231		211	6 feet 11 inches	83
107	236				
109	240				
111	245				
113	249				
115	254				
117	258				
119	262				

APPENDIX C
DATA PROTECTION

C-1. GENERAL

"Installation Access Control System (IACS)" (glossary) data contains personally identifiable information. The use and release of IACS data is governed by DOD 5400.11-R and the Privacy Act of 1974, and by applicable host nation (HN) data protection standards. IACS data may only be released for official investigations, not for internal organization or unit investigations. The data is protected and must not be used for administrative purposes such as tracking individuals; enforcing base restrictions; serving as a time clock; issuing drug testing notifications; or enforcing payment of traffic, phone, utilities, or other debts.

C-2. RELEASE OF IACS DATA

a. IACS data may be approved for release under very limited conditions. Examples are as follows:

(1) Data is required by law based on an appropriate legal review.

(2) A law enforcement (LE) agency (for example, a U.S. agency, an HN agency, INTERPOL) requests IACS data in support of an ongoing investigation.

(3) IACS data is requested by an authorized DOD or HN organization (for example, the DOD Inspector General (IG), the Army Audit Agency (AAA), a HN tax investigation office). Relevant IACS data may be provided to a properly detailed investigating officer under AR 15-6.

b. Requests submitted by HN organizations must be validated by a DOD representative or agency acting as an intermediary for the request. IACS users other than authorized LE personnel will not release data directly to HN representatives.

C-3. IACS DATA REQUESTS FOR INFORMATION (RFIs)

a. IACS data RFIs will—

(1) Be submitted in writing.

(2) Be sent by encrypted email to the responsible "military police (MP)" (glossary) desk for a law enforcement operator (LEO) to conduct the lookup.

(3) Include an investigation number with a brief description of the investigation. If the investigation is preliminary and an investigation number has not been assigned, the request must include an explanation of why the "requester" (glossary) believes the information should be provided. Such cases require a legal review by the Office of the Judge Advocate, HQ USAREUR-AF, before data is released.

(4) If submitted by an authorized DOD organization, include a brief statement defining the tasking authority (for example, the Secretary of the Army tasking the AAA or the IG to conduct an audit).

b. RFIs that exceed the standard reports available to the LEO require a trouble ticket submitted to the Defense Manpower Data Center Helpdesk.

C-4. UNIQUE RFIs

a. Authorized LE or other organizations will send unusual or unique RFIs to their appropriate legal office for a formal legal opinion.

b. Extensive RFIs may require a search warrant. Requesters will contact their responsible legal office for guidance on how to submit a search warrant request to the acting magistrate or HN court.

C-5. UNACCEPTABLE RFIs
The following are examples of unacceptable RFIs that must not be completed:

a. An RFI to determine if an individual broke base restrictions.

b. An RFI submitted by a supervisor who wants to know when an employee entered the base (time clock stamp).

c. An RFI submitted by an individual who wants to track Family or spouse movements.

C-6. ACCEPTABLE RFIs
The following are examples of acceptable RFIs:

a. An RFI relating to a felony or serious crime committed on an installation.

b. An RFI supporting an attempt to locate a missing or runaway child.

c. An RFI relating to a Servicemember who has been documented as being absent without leave.

d. An RFI submitted by the Trial Counsel, the Criminal Investigation Division, or MP in support of a court-martial.

APPENDIX D
PRIVACY ACT STATEMENT FOR U.S. CITIZENS AND LAWFUL PERMANENT RESIDENTS

IACS Privacy Act Statement for DBIDS (For U.S. Citizens and Lawful Permanent Residents)

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DOD Instruction (DODI) 1000.25, DOD Personnel Identity Protection (PIP) Program; DODI 5200.08, Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB); DOD 5200.08-R, Physical Security Program; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): To provide necessary information to DOD installations to determine if applicant meets access control requirements. Use of SSN is necessary to make positive identification of an applicant. Records in the DBIDS system are maintained to support Department of Defense physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the DOD, and for producing facility management reports. Used by security offices to monitor individuals accessing DOD installations and/or facilities. SSN, Driver's License Number, or other acceptable identification will be used to distinguish individuals who request entry to DOD installations and/or facilities.

ROUTINE USE(S): To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature. The remaining routine uses can be found in the applicable system of records notice, DMDC 10 DOD, Defense Biometric Identification Data System (DBIDS), located at *http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570565/dmdc-10-dod/*.

DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial of a DBIDS card or pass and denial of entry to DOD installations and/or facilities.

APPENDIX E
ADJUDICATION STANDARDS AND PROCEDURES USING BACKGROUND CHECKS

E-1. PURPOSE
This appendix establishes the minimum adjudication standards to be used by "area commanders" (glossary) and host nation (HN) base commanders when determining an individual's fitness to access an installation. The purpose is to standardize the review of adverse information within the USEUCOM area of responsibility. U.S. and HN base commanders may add to these standards.

E-2. REFERENCES

a. DOD Manual 5200.08, Volume 3.

b. AD 2014-05, enclosure 2.

c. AEA Reg 27-9.

d. AEA Reg 27-10.

NOTE: References are listed in appendix A.

E-3. POLICY
For individuals requesting a pass that requires a background check, area commanders will incorporate the following assessment areas as minimum standards to their adjudication program and deny access to military installations when adverse information in subparagraphs a through i below has been identified.

a. Terrorism. The individual has actively or passively participated in terrorist activities (for example, in the areas of recruiting, funding, supplying, aiding, or making terrorist threats).

b. Debarment. The individual is barred by a commander.

c. Use of Lost, Stolen, or Fake Identification. The individual attempted to use or has used a lost, stolen, or fabricated identification to gain access to an installation.

d. Criminal Conviction.

(1) The individual has a criminal conviction for any of the following: armed assault, armed robbery, arson, assault with a deadly weapon, child molestation, drug distribution or drug possession with intent to sell, espionage, firearms or explosives violations, murder, production or possession of child pornography, rape, sabotage, sexual assault, trafficking in humans, transporting radioactive material, or treason.

(2) In the past 10 years, the individual had a criminal conviction for any of the following: burglary, unlawful entry, or housebreaking; grand theft auto; or involuntary or vehicular manslaughter.

(3) In the past 5 years, the individual had a criminal conviction for any of the following: habitual drug offense (for example, use of marijuana), forgery, or fraud.

e. Felony Conviction. In the past 10 years, the individual had a felony conviction (regardless of the type of offense or violation).

f. Arrest Warrant. The individual has a current U.S., HN, or INTERPOL arrest warrant.

g. Engagement in Activities Designed to Overthrow a Government. The individual has engaged in acts or activities designed to overthrow the U.S. Government, the government of a "European Union" (glossary) or NATO member state, or the HN government by force.

h. Sexual Offense. The individual is a registered sex offender.

i. Criminal Arrest. A background check revealed criminal arrest information about the individual that causes the installation commander to determine that the individual presents a potential threat to the good order, discipline, health, or safety of the garrison. The commander will bar the individual in accordance with "component" (glossary) regulations, such as AEA Regulation 27-9 or AEA Reg 27-10, as applicable.

E-4. PROCESSING REQUESTS FOR A WAIVER OF ACCESS DENIAL

a. Individuals who want to request a waiver of their access denial that resulted from adverse information revealed during a background check must send a personal letter with a return address through the civilian misconduct office to the installation commander in English (for individuals in Italy, also in Italian for the Italian base commander) stating why their conduct should not result in denial of access.

b. The following information should be included in or be attached to the letter:

(1) Specific circumstances surrounding the conduct or incident.

(2) The length of time elapsed since the conduct or incident.

(3) The age of the individual at the time of the conduct or incident.

(4) Proof of efforts toward rehabilitation.

(5) Remorse for the conduct or incident.

(6) Letters of recommendation or character references from previous employers.

(7) A letter or memorandum from the sponsor supporting the request for a waiver.

b. Commanders will review individual packets and determine whether or not to overturn their access denial decision.

c. If a commander's review results in no change to the denial, a letter will be sent to the individual stating the following: "In response to your request, I conducted a review of the available records and determined that no changes or corrections are warranted at this time. Please do not attempt to enter any U.S. or host-nation military installations again."

d. If a commander grants a waiver to the debarment, the civilian misconduct office will send a copy of the waiver to the Office of the Provost Marshal, G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF, to update the individual's "Installation Access Control System" (glossary) record.

APPENDIX F
DEBARMENT

F-1. REFERENCES

a. AEA Reg 27-9.

b. AEA Reg 27-10.

c. Applicable host nation technical agreements.

F-2. POLICY

"Area commanders" (glossary) are barring authorities for their installations.

F-3. PLACING A BAR IN THE INSTALLATION ACCESS CONTROL SYSTEM

a. Debarments cannot be entered locally by the base security officer, the site security manager, or the law enforcement operator. They must be sent to the Office of the Provost Marshal (OPM), G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF, for processing and placement in the "Installation Access Control System (IACS)" (glossary).

b. All debarment memorandums will be sent to OPM at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil* for entry into IACS.

F-4. REDRESS

Individuals who want to "redress" (glossary) their debarment must contact the barring authority, normally the area commander.

F-5. LIFTING A DEBARMENT IN IACS

The signed area commander memorandum removing a bar must be sent to OPM at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@army.mil* to have the bar lifted in IACS.

APPENDIX G
USEUCOM WATCHLISTING

G-1. PURPOSE
This appendix describes the use of the "Installation Access Control System (IACS)" (glossary) Enhanced Screening Watchlist function to prevent non-DOD-affiliated persons from obtaining a visitor pass or a regular pass.

G-2. REFERENCE
Homeland Security Presidential Directive 6, Integration and Use of Screening Information to Protect Against Terrorism.

G-3. POLICY

a. The Office of the Provost Marshal (OPM), G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF, is responsible for USEUCOM Watchlist operations.

b. OPM places individuals identified as unfit for installation access by a nominating agency (for example, National Ground Intelligence Center, INTERPOL, FBI, Office of Special Investigations, Military Intelligence, Navy Crime Investigative Service, USAREUR-AF G2X) on the Watchlist.

c. Nominating agencies will send their nominations to OPM through secure means based on the level of classification.

G-4. REDRESS
Individuals who want to "redress" (glossary) their access denial due to their placement on the Watchlist may request AEA Form 190-16G from the gate guard or "registrar" (glossary). OPM will coordinate the review of the information provided on AEA Form 190-16G and will reply in a memorandum to the individual stating one of the following:

a. After a review of all available records, a determination was made that no changes or corrections to the access denial are warranted. Do not attempt again to enter any U.S. military installations or host nation military installations where U.S. forces are stationed.

b. After a review of all available records, a determination has been made that similar data matches were occurring between your personal data and that of an individual who was identified as not authorized on any installation. A determination was made to remove your access denial.

c. After a review of all available records, a determination was made to remove your access denial.

APPENDIX H
LAW ENFORCEMENT OPERATORS

H-1. GENERAL
The "Installation Access Control System (IACS)" (glossary) law enforcement operator (LEO) role is critical in the "encounter management" (glossary) process when IACS provides an alert to the guard and when placing law enforcement (LE) flags in IACS. Individuals given the LEO role in IACS will follow the detailed LEO standard operating procedures (SOPs) in IACS Policy Memorandum #4, Encounter Management, posted on the IACS portal at *https://armyeitaas.sharepoint-mil.us/sites/USAREUR-AF_OPM_IACS*.

H-2. ENCOUNTER MANAGEMENT
When the Defense Biometric Identification System (DBIDS) detects a match with an adverse record, it will display an alert message (table 1). The LEO must be trained and proficient in conducting a DBIDS lookup, and must process the information to provide the correct guidance to the "access control point (ACP)" (glossary) guard. If required, the LEO will dispatch "military police (MP)" (glossary) to the ACP and, if non-U.S. citizens are involved, notify local host nation (HN) LE if appropriate.

H-3. FLAGGING AN INSTALLATION PASS OR VISITOR PASS AS LOST OR STOLEN
Individuals are required to report to the MP station when their "installation pass" (glossary) or visitor pass is lost or stolen. On receipt of the report, the LEO is required to flag the credential immediately as lost or stolen. Once an installation pass or visitor pass is flagged as lost or stolen, it cannot be reactivated.

NOTE: Individuals whose DOD ID card is lost or stolen are required to report immediately to the closest Defense Enrollment Eligibility Reporting System (DEERS)/Real-Time Automated Personnel Identification System (RAPIDS) office, which will terminate the DOD ID card. The IACS will receive the update automatically from DEERS/RAPIDS.

H-4. ASSIGNING A LAW ENFORCEMENT STATUS BY FLAGGING AN IACS RECORD

a. There are two types of LE statuses: Warning and Adverse.

(1) Warning Flags. IACS includes two warning flags that alert ACP guards with a yellow banner on their IACS scanners (fig 4). The two warning flags are as follows:

(a) Barred at Other Bases. The ACP guard will deny access unless the individual has an "area commander" (glossary) adjudication memo.

(b) Driving Status Suspended. Use this flag for individuals who have received formal written notification that their driving status has been suspended. If an individual is driving a vehicle, the ACP guard will stop the individual and contact the MP desk. If the individual is a passenger and is not driving the vehicle, the individual will be allowed to access the installation.

(2) Adverse Flags.

(a) Adverse flags alert ACP guards with a red banner on their IACS scanners (fig 4) requiring guards to deny installation access. ACP guards will contact the MP desk and provide the details of the adverse flag. The Office of the Provost Marshal (OPM), G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF, enters the adverse "Barred" flag into IACS on receipt of the area commander's debarment memo. The "Access denied at this FPCON level" and "Access denied at this HPCON level" flags are entered by the base security officer in accordance with IACS Policy Memorandum #5. A match against the DOD Identity Matching Engine for Security and Analysis (IMESA) will automatically generate the following flags: Wants Warrant Hold, Sex Offender Registration Alert, and Violent Person. The IACS software displays the following flags based on individual situations: Sponsor no longer valid, Expired ID card, Access not authorized at this time, Access not authorized on this day, Access denied at this FPCON level, Access denied at this HPCON level.

(b) The IACS includes the following eight adverse flags that LEOs can use:

1. Armed and Dangerous. Use this flag to temporarily deny access if there is probable cause that an individual has weapons and intends to attack a U.S., NATO, or HN installation. Remove the flag when the individual is no longer a threat (for example, has been arrested). Information on individuals who are not in IACS and have weapons for the purpose of attacking U.S., NATO, or HN installations should be forwarded to OPM to be added to the USEUCOM Watchlist (app G).

2. BOLO. Use the "Be on the Look Out" (BOLO) flag when information is received from an authorized LE source (for example, FBI, Office of Special Investigations, Criminal Investigation Division, Navy Crime Investigative Service). Remove the flag on expiration of the BOLO status.

3. Call Law Enforcement. Use this flag for LE purposes.

4. International Hold. Use this flag when notified by HN LE.

5. Missing. Use this flag to locate missing dependents.

6. Site Suspension. Use this flag temporarily to deny installation access to a person pending area commander debarment.

7. Unauthorized Absence. Only use this flag when an individual's unit officially submitted the absent without leave (AWOL) (UCMJ Article 86) status to the respective Service agency. Do not use this flag, for example, if a unit reports an individual as late, or as not showing up for work, formation, or duty. After 30 days, update the flag from AWOL to Deserter status. Remove the flag when the individual returns or is incarcerated.

8. Wants Warrant Hold. Use this flag to arrest an individual.

b. IACS Policy Memorandum #4, Encounter Management, appendixes A and B, provides more detailed procedures for flagging an individual in IACS for law enforcement purposes.

APPENDIX I
INSTALLATION PASS CATEGORIES

NOTE: The glossary defines acronyms and terms used in the table below.

Table I-1
Installation Pass Categories

CATEGORY	Expiration Period	Requesting Authority	Background Check	Residence or Work Permit	Authorized Access Level	Authorized Days/Times	Sponsor Privileges Authorized	FPCON Restriction
Conveyance (para 16)	Max 3 years	Sponsoring organization	*Yes	May be required	Limited to minimum required	Limited to minimum required	Varies	**B
Facility Use/Vendor (para 17)	Max 1 year	IACO, AAFES, DeCA, or IMCOM-E	Yes	Yes, for non-EEA citizens	Limited to listed installations	Limited to minimum required	No	B
Foreign Civilian Visitor (para 18)	Max 1 year	Requesting organization	As determined by commander or commander's designee	N/A	Limited to minimum required for visit	Limited to minimum required for visit	No	*B
Foreign Government Civilian/Local National Employee (para 19)	Max 3 years	Requesting organization or supervisor	*Yes – initial pass *No – renewal	N/A	Limited to minimum required for position	Limited to minimum required for position	Yes, if sponsor provides justification	**B
Foreign Government Contractor (para 20)	Max 3 years	COR or alternates	Yes	Yes, for non-EEA citizens	Limited by contract or PWS	Limited by contract or PWS	Yes, if sponsor provides justification	**B
Foreign Military/Foreign Military Dependent (para 21)	Max 3 years	Requesting organization	No	No	Limited by duty location and HN country	Limited per sponsor justification	Yes	D
Long-Term Visitor (para 22)	Max 1 year	ID cardholder (over 18)	Yes	Yes, for non-EEA citizens after 90 days	Limited to where requester resides	Limited per sponsor justification	No	B
Personal Delivery (Recurring Deliveries or Similar Services Not Associated With a Government Contract) (para 23)	Max 1 year	Sponsoring Organization	Yes	Yes, for non-EEA citizens	Limited to service area	Limited to service hours	No	B

Table I-1
Installation Pass Categories—Continued

CATEGORY	Expiration Period	Requesting Authority	Background Check	Residence or Work Permit	Authorized Access Level	Authorized Days/Times	Sponsor Privileges Authorized	FPCON Restriction
Personal Services (para 24)	Max 1 year	IACO	Yes	Yes, for non-EEA citizens	Limited to requester installation	Limited by contract	No	B
Privatized Housing (para 25)	Max 3 years	Requesting Organization or POC	No	No	Installation of residence or private land	24/7	Yes, with limits	D
U.S. Government Contractor (Non-CAC holder) (para 26)	Max 1 year	COR or Alternate	Yes, U.S. only	May be required, or BACO-90	Limited by contract or PWS	Limited by contract or PWS	No, unless sponsor justifies	**B
Volunteer (para 27)	Max 1 year	Requesting Organization	Yes	Yes, for non-EEA citizens after 90 days	Limited to service area	Limited to service hours	No	B
Other (para 28)	Max 1 year	Requesting Individual	Yes	Yes, for non-EEA citizens after 90 days	Limited to minimum required	Limited to minimum required	No	B

*** Some exceptions apply.**
**** "Essential personnel" (glossary) may get FPCON C or D access.**

GLOSSARY

SECTION I
ABBREVIATIONS

24/7	24 hours a day,7 days a week
AAA	Army Audit Agency
AAFES	Army and Air Force Exchange Service
ACOR	alternate contracting officer's representative
ACP	access control point
AD	Army directive
AE	Army in Europe
AEA	Army in Europe and Africa
AEPUBS	Army in Europe and Africa Publications [website]
AFMAN	Air Force manual
AOR	area of responsibility
app	appendix
AR	Army regulation
AT	antiterrorism
AWOL	absent without leave
BOLO	Be on the Look Out
BSO	base security officer
BX	base exchange
CAC	common access card
CNE-CNA-C6F	Commander, U.S. Naval Forces Europe/Commander, U.S. Naval Forces Africa/Commander, U.S. Sixth Fleet
CNIC-M	Commander, Navy Installations Command, manual
CNREURAFCENT	Commander, Navy Region Europe, Africa, Central
CNREURAFCENT N34	Physical Security, Navy Region Europe, Africa, Central
COR	contracting officer's representative
DA	Department of the Army
DAF	Department of the Air Force
DBIDS	Defense Biometric Identification System
DD	Department of Defense [form]
DeCA	Defense Commissary Agency
DEERS	Defense Enrollment Eligibility Reporting System
DES	director of emergency services
DOCPER	Department of Defense Contractor Personnel Office, Civilian Personnel Directorate, Office of the Deputy Chief of Staff, G1, Headquarters, United States Army Europe and Africa
DOD	Department of Defense
DODM	Department of Defense manual
E-7	sergeant first class
E-8	master sergeant/first sergeant
EEA	European Economic Area
ETP	exception to policy
EU	European Union
FBI	Federal Bureau of Investigation
fig	figure

FPCON	force protection condition
GCC	Good Conduct Certificate
GS	General Schedule
HAV	heavy armored vehicle
HN	host nation
HPCON	health protection condition
HQ USAREUR-AF	Headquarters, United States Army Europe and Africa
HSPD	Homeland Security Presidential directive
IACO	installation access control office
IACP	Installation Access Control Program
IACS	Installation Access Control System
ID	identification
IG	inspector general
IMCOM-E	United States Army Installation Management Command Europe
JIAWG	Joint Installation Access Working Group
LE	law enforcement
LEO	law enforcement operator
LN	local national
LNSP	Local National Screening Program
max	maximum
mil	military
MIPR	military interdepartmental purchase request
MP	military police
MRZ	machine-readable zone
NATO	North Atlantic Treaty Organization
NCIC	United States National Crime Information Center
NCIC III	United States National Crime Information Center Interstate Identification Index
NOK	next of kin
O-1	second lieutenant
O-3	captain
O-5	lieutenant colonel
OCONUS	outside the continental United States
OPM	Office of the Provost Marshal, G34 Protect, Office of the Deputy Chief of Staff, G3, HQ USAREUR-AF
OPORD	operation order
para	paragraph
PDA	personal digital assistant
PII	personally identifiable information
PL	public law
PO	private organization
POC	point of contact
PR&C	purchase request and commitment
PWS	performance work statement
PX	post exchange
RAPIDS	Real-Time Automated Personnel Identification System
RFI	request for information
SAFE	[Department of Defense] Secure Access File Exchange
SAV	staff assistance visit

SCOR	site contracting officer's representative
SECO	security officer
SEV	security escort vehicle
SF	standard form
SFS	security forces squadron
SOFA	[North Atlantic Treaty Organization] Status of Forces Agreement
SOP	standard operating procedure
SSN	Social Security number
TT	Trusted Traveler
TV AL II	*Tarifvertrag vom 16. Dezember 1966 für die Arbeitnehmer bei den Stationierungsstreitkräften im Gebiet der Bundesrepublik Deutschland*
UCMJ	Uniform Code of Military Justice
U.S.	United States
USAFE/AFAFRICA	United States Air Forces in Europe/United States Air Forces Africa
USAFE/AFAFRICA A4	Logistics, Engineering, and Force Protection, United States Air Forces in Europe/United States Air Forces Africa
USAFE/AFAFRICA A4S	Security Forces, United States Air Forces in Europe/United States Air Forces Africa
USAG	United States Army garrison
USAREUR-AF	United States Army Europe and Africa
USAREUR-AF G2	Deputy Chief of Staff, G2, United States Army Europe and Africa
USAREUR-AF G2X	Deputy Chief of Staff, G2, United States Army Europe and Africa
USAREUR-AF G3	Deputy Chief of Staff, G3, United States Army Europe and Africa
USAREUR-AF G6	Deputy Chief of Staff, G6, United States Army Europe and Africa
USAREUR-AF PM	Provost Marshal, United States Army Europe and Africa
USC	United States Code
USEUCOM	United States European Command
USEUCOM J34	Joint Protection Division, United States European Command
VA	United States Department of Veterans Affairs
VHIC	Veterans Health Identification Card
VIP	very important person
W-2	chief warrant officer 2
W-3	chief warrant officer 3

SECTION II
TERMS

access control point
Referred to as a gate or an entry control point

access roster
A list of individuals authorized unescorted short-term access to an installation

applicant
An individual applying for installation access

application
AEA Form 190-16A used to apply for access to U.S. Forces installations in Europe

area commanders
United States Army garrison commanders, USAFE/AFAFRICA commanders, CNREURAFCENT commanders, and host nation commanders (as applicable, based on agreements between the United States and HNs)

Aufenthaltstitel
Document issued in Germany to individuals who are not citizens of a European Union (EU) member state or of one of the other states of the European Economic Area (that is, Iceland, Liechtenstein, or Norway) and who want to reside, or to reside and work in Germany temporarily or permanently. This document is issued either as a temporary visa, *Aufenthaltserlaubnis*, or EU Blue Card, or as a permanent *Niederlassungserlaubnis* or *Erlaubnis zum Daueraufenthalt–EU*. If authorization to work has been granted, the *Aufenthaltstitel* will explicitly indicate so.

carta d'identità
The Italian national identity card

carte d'identité
The French name for the Belgian national identity card

category
Any one of 13 designations of individuals registered in the Installation Access Control System. Each category has specific risk-based registration requirements and restrictions based on the relationship between the individual and the U.S. Forces.

component
One of the Service branches or commands in the United States European Command area of responsibility: Army or USAREUR-AF; Air Force or USAFE/AFAFRICA; Navy or CNREURAFCENT.

contractor
An individual working under contract for the DOD. This includes primary contractors, subcontractors (individuals contracted by the primary contractor to perform portions of a contract), and individual contractors.

Defense Biometric Identification System (DBIDS) Card
The access card produced by the DBIDS and issued to non-DOD ID cardholders, also referred to as an installation pass

encounter management
A process that begins at the access control point (ACP) when the Installation Access Control System alerts the guard with a yellow or red response. The ACP guard will follow the directions in table 1 of this publication.

essential function
A function that if not performed would seriously affect a unit or its mission

essential personnel
Personnel who are authorized access to an installation during force protection condition Charlie because of the services they provide

European Economic Area
The 27 European Union countries plus Iceland, Liechtenstein, and Norway

European Union
The countries of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden

first or emergency responder
An individual who is authorized access to an installation during force protection condition Delta because of the services that the individual provides

Identiteitskaart
The Flemish name for the Belgian national identity card

in loco parentis
(Latin, "in the place of a parent")
The legal situation under which an individual temporarily assumes parental rights, duties, and obligations without going through the formalities of legal adoption

installation access control office
An office authorized to register individuals in the Installation Access Control System and to produce and issue installation passes and access rosters

Installation Access Control System
The personnel access verification system that is used to manage the Installation Access Control Program in the European theater

installation pass
The access card produced by the Defense Biometric Identification System (DBIDS) and issued to non-DOD ID cardholders, also referred to as a DBIDS Card

Local National Screening Program
A USAREUR-AF G2 program, described in AEA Reg 604-1, to conduct German background checks on German citizens and legal residents

military police
An umbrella term for military law enforcement officers, including U.S. Air Force security forces and U.S. Navy masters-at-arms.

redress
A request for reconsideration of installation access submitted by an individual who was denied access to an Army installation because of lack of personal information or adverse results of a background check

registrar
An official who is authorized to register individuals in the Installation Access Control System (for example, by registering individuals' DOD ID cards), issue installation passes, and create access rosters

requester
An individual cardholder who is authorized to request an installation pass, but is not authorized to perform sponsoring organization responsibilities. The requester status applies only to the *Long-Term Visitor* category (para 22), the *Personal Services* category (para 24), and the *Other* category (para 28).

sponsoring official
An individual who represents a sponsoring organization and carries out the organization's sponsoring responsibilities

Trusted Traveler (TT)
A program that installation commanders may implement in accordance with the USEUCOM antiterrorism operation order, under which DOD ID cardholders registered in the Installation Access Control System are authorized to vouch for passengers in their vehicles that have a valid form of photo ID. TT procedures must not be used during force protection conditions Charlie and Delta.

unserviceable
Any condition or change to a DOD ID card or installation pass that impairs a guard's ability to verify that the cardholder is the individual on the card or pass, or that causes the guard to question whether the card has been altered. "Unserviceable" does not include minor bends, peeled lamination, fading print, or other deficiencies that do not impair a guard's ability to verify that the cardholder is the individual indicated.

visitor sponsor privileges
Privileges granted to certain categories of individuals that allow those individuals to escort visitors after they have been issued a visitor pass