Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command
Europe
Sembach, Germany

Army in Europe
Regulation 190-16*

27 April 2017

Military Police

Installation Access Control

***This regulation supersedes AE Regulation 190-16, 11 January 2010.**

The English version of this regulation is the governing directive for all categories of personnel except for personnel employed under the provisions of the *TV AL II*.

For the Commander:

KAI R. ROHRSCHNEIDER
Brigadier General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes policy and procedures for controlling access to U.S. Forces installations in Europe. It does not apply to restricted areas governed by other regulations (AR 190-13).

Summary of Change. This revision completely revises the previous edition of the regulation.

Applicability. This regulation applies to personnel 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 conjunction with the standing operating procedure on contingency-base access control issued by the Office of the Provost Marshal, HQ USAREUR (OPM), incorporating local procedures.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are on the Army Records Information Management System website at *https://www.arims.army.mil*.

Supplementation. Organizations will not supplement this regulation without OPM approval. United States Army garrisons in Belgium, Italy, and the Netherlands may, however, develop policy and procedures that meet or exceed the standards of this regulation to meet their unique needs.

Forms. This regulation prescribes AE Form 190-16A, AE Form 190-16B, AE Form 190-16C, AE Form 190-16E, AE Form 190-16F, AE Form 190-16G, AE Form 190-16H, AE Form 190-16I, AE Form 190-16K. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at *http://www.eur.army.mil/aepubs/*.

Suggested Improvements. The proponent of this regulation is the Installation Access Control System (IACS) Program Office, OPM (mil 537-7427). Users may send suggested improvements to this regulation by e-mail to the IACS Program Office at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@mail.mil*.

Distribution. This regulation is available only electronically and is posted in AEPUBS at *http://www.eur.army.mil/aepubs/*.

CONTENTS

SECTION I
GENERAL

1. PURPOSE
This regulation—

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

b. Provides IACS registration procedures.

c. Provides procedures for preparing and issuing installation passes.

d. Must be used with the following publications (app A):

(1) Army Directive (AD) 2014-05.

(2) AR 25-400-2.

(3) AE Regulation 25-400-2.

(4) AE Regulation 190-13.

(5) AE Regulation 525-13.

(6) AE Regulation 600-700.

(7) AE Regulation 604-1.

(8) AE Regulation 715-9.

2. REFERENCES
Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS
The glossary defines abbreviations and terms.

4. GENERAL

a. This regulation prescribes installation-access-control policy and provides procedures for personnel verification. AE Regulation 190-13 provides information on the physical design of access-control points (ACPs). This information may also be obtained from installation antiterrorism officers, physical-security officers, and the Director of Emergency Services, United States Army Installation Management Command Europe (IMCOM-Europe).

b. The IACS provides—

(1) An additional layer of security by minimizing access to installations by individuals using a forged, stolen, or lost DOD ID card or installation pass.

(2) The ability to implement force-protection measures USAREUR- and USAFE-wide or at the garrison or installation level based on the force-protection condition (FPCON).

(3) A centralized control of access privileges (for example, sponsors may withdraw the access authorization of a terminated employee, commanders may bar individuals, desk sergeants using the IACS Law Enforcement Official (LEO) module may flag individual IACS records).

c. Individual access privileges are risk-based and depend on an individual's category (glossary) (paras 11 thru 27).

5. RESPONSIBILITIES

a. USAREUR G2. The USAREUR G2 will—

(1) Manage the German Local National Screening Program (LNSP) (glossary) in accordance with AE Regulation 604-1.

(2) Provide an automated online system to support the LNSP program.

b. USAREUR G3/5/7. The USAREUR G3/5/7 will coordinate changes to—

(1) AE Regulation 525-13 concerning installation access during elevated FPCONs.

(2) AE Regulation 525-50 concerning installation access for inspection teams.

c. Office of the Provost Marshal, HQ USAREUR (OPM). The OPM will—

(1) Provide staff supervision and direction for the Installation Access Control Program (IACP).

(2) Be the proponent for installation-access-control policy and the IACS. This includes system fielding, testing, life-cycle-replacement management, and operator training.

(3) Be the approving authority for written requests for exception to policy (ETP).

(4) Coordinate access-authorization decisions with sponsoring organizations for all installation-pass applications when the results of any background check show adverse information and access to more than one United States Army garrison (USAG) is requested.

(5) Conduct staff-assistance visits to review IACS registration and installation-pass issuing procedures.

(6) Ensure all installation access control offices (IACOs) (glossary) comply with regulatory requirements.

(7) Perform automated audits on IACS user activity.

(8) Coordinate with IMCOM-Europe and USAGs to ensure that the IACS database accurately shows all barred individuals.

(9) Be responsible for the USAREUR encounter-management program (glossary).

(10) Be the adjudication authority for requests for redress of access denial (AE Form 190-16G) and issue the appropriate response (AE Form 190-16H or AE Form 190-16I) based on the decision.

(11) Provide required reports on USEUCOM-wide bars in accordance with AE Regulation 27-9, figure C-1.

(12) Coordinate USAREUR-wide access authorization when an IACS application (glossary) submitted by USAFE/AFAFRICA requests access to more than one USAG.

d. USAG Commanders. USAG commanders will—

(1) Develop policy to ensure access to installations within their garrisons is controlled in accordance with this regulation.

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

(3) 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.

(4) Serve as senior officials for making fitness determinations and adjudicating on an individual's access in accordance with AD 2014-05 when the background check of an installation-pass applicant reveals adverse information. USAG commanders may designate personnel in writing to make fitness determinations. USAG commanders and their designated appointees will use the adjudication standards in appendix E to make fitness determinations and adjudicate on an individual's access. If an applicant requests access to more than one USAG and the USAG commander recommends approval, the USAG will send the request by encrypted e-mail to the OPM at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@mail.mil* for adjudication.

(5) Notify the OPM (*usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@mail.mil*) and the IACS Help Desk (*usarmy.badenwur.usareur.list.opm-iacs-help-desk@mail.mil*) by e-mail of all USAG- and Army-in-Europe-wide bars.

(6) Perform sponsoring-organization responsibilities where this regulation designates the USAG as the sponsoring organization.

(7) Consult the OPM on access options when the access requirements in paragraph 8 do not adequately support co-use agreements with the host nation (HN).

(8) Provide a copy of the USAG ACP policy to the responsible works council.

e. USAG Commanders in Belgium, Italy, and the Netherlands. In addition to performing the responsibilities in subparagraph d above, USAG commanders in Belgium, Italy, and the Netherlands will adapt the policy and procedures in this regulation to meet unique HN laws as needed (for example, requirements for background checks, obtaining fingerprints, vehicle registration, residence and work permits). The adapted policy and procedures must—

(1) Meet or exceed the security standards and intent of this regulation whenever possible.

(2) Be coordinated with and approved by the OPM and the USAREUR Judge Advocate.

f. USAG Directors of Emergency Services. USAG directors of emergency services will—

(1) On receipt of notification that a DOD ID card or installation pass has been lost or stolen, immediately flag the record in the IACS to deregister the lost or stolen card or pass.

(2) Develop procedures to support law-enforcement background checks required for installation passes. Copies of law-enforcement background-check results must be sent to the sponsoring organization. When the results include adverse information, copies must be sent to the sponsoring organization and the USAG. USAG policy for processing background checks that resulted in adverse information must be followed.

(3) Authorize and remove access to the IACS for site security managers (SSMs), LEO module operators, and registrars (glossary) using DD Form 2875. Directors of emergency services will post DD Form 2875 to the USAG directorate of emergency services (DES) tab on the IACS portal. Directors of emergency services are responsible for informing OPM when to revoke access to the IACS.

(4) Appoint at least a primary and alternate IACS SSM and ensure SSMs conduct regular and recurring inspections of IACS equipment, submit trouble tickets as required, and maintain OPM's hand-receipts on IACS equipment.

(5) Enforce removal of visitor-sponsor privileges (glossary) for violating the physical-escort policy (paras 36b(5) and 36e).

(6) Ensure every USAG ACP has an adequate supply of AE Form 190-16B and AE Form 190-16G, and paper and toner for printing the escorted-visitor paper pass.

(7) Ensure all IACS users, including sponsors, complete the required IACS training in accordance with the IACS standing operating procedure (SOP) posted on the IACS portal.

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

(9) Ensure ACP guards provide AE Form 190-16B to individuals whose installation pass or DOD ID card is confiscated.

g. Contracting Offices. Contracting offices awarding contracts for supplies to be delivered to or for work to be performed on U.S. Forces-controlled installations will—

(1) Ensure contracts include requirements for background checks and, if necessary, valid residence and work permits required for issuing installation passes to contractor (glossary) employees or including contractor employees on access rosters in accordance with this regulation.

NOTE: Citizens of a country of the European Economic Area (EEA) (that is, EU member countries, Iceland, Liechtenstein, and Norway) normally do not require a residence or work permit for staying and working in another EEA country. In Germany, individuals who are not citizens of a country of the EEA generally require a residence permit (*Aufenthaltstitel* (glossary)). If permission to work has been granted, the *Aufenthaltstitel* will explicitly indicate the authorization and its extent. Separate work permits are no longer issued by German authorities.

(2) Include a provision in contracts to ensure that contractors return all installation passes to the issuing IACO when the contract is completed or when a contractor 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 requiring activities (RAs) requesting contract services include the required information (j(5)(a) and (b) below) 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.

h. Army Reserve Major Subordinate Commands. Army Reserve major subordinate commands will develop procedures for screening all troop program unit (TPU) Soldiers and Family members to ensure they meet HN residency requirements as needed (that is, requirements for an *Aufenthaltstitel* in Germany or a *Permesso di Soggiorno* in Italy). As a minimum, Army Reserve units in Europe will provide the USAREUR IACS Program Manager the following:

(1) On a semiannual basis, a list of all assigned TPU Soldiers and Family members who reside in the EU and require IACS registration. The list will include a certification from the command confirming that the command has ensured that individuals listed have the proper HN residency documentation or the appropriate status under the NATO Status of Forces Agreement (SOFA).

(2) Notification within 30 days after a change in status of any assigned Soldier or Family member on the list (for example, transferring out of the unit, voluntarily or involuntarily separating from the Army Reserve, obtaining independent NATO SOFA status).

i. IACOs. Section V explains IACO responsibilities.

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

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

(2) An installation-pass application (glossary) (AE Form 190-16A) is prepared for each installation-pass applicant. The application will identify an applicant's access requirements and justify these requirements in accordance with this regulation (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 host USAG commander or, if USAREUR-wide access is requested, with the OPM to determine if the adverse information warrants denial of the request.

(4) Installation-pass applicants register their privately owned vehicles (POVs) in accordance with the procedures in this regulation and AE Regulation 190-1 (when applicable). Vehicle registration is required for all installation-pass applicants who use a POV to enter U.S. Forces installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

(5) The following information is included on all PR&Cs, MIPRs, and other requests for contracting support when the contract will result in contractors requiring access to U.S. Forces installations:

(a) The name of the sponsoring organization and the name and telephone number of its installation-access POC.

(b) The location of the responsible IACO and the name and telephone number of the IACO POC.

(6) Contracting officers (KOs) outside the purview of the 409th Support Brigade (Contracting) are informed of the installation-access policy in this regulation.

(7) Issued installation passes are retrieved and returned to the issuing IACO when the relationship that served as the justification for the installation pass changes or is terminated.

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

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

(10) A record of personnel sponsored by the organization and supporting documentation is maintained.

(11) A reconciliation of U.S. Forces in Europe 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.

(12) DD Forms 577 that designate persons authorized to perform sponsoring-official (glossary) duties on behalf of the sponsoring organization (para 28a(2)(b)) are sent to the servicing IACO and updated annually.

(13) The procedures in paragraph 28b(8) are followed when the sponsoring official cannot escort an applicant to the servicing IACO.

(14) They complete mandatory IACS sponsor training through AKO to qualify as a sponsor.

(15) 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).

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

(1) Consent to the procedures for obtaining digitized fingerprint minutia data (DFMD) when—

(a) Inprocessing. Persons with an authorized, machine-produced DOD ID card will provide DFMD while inprocessing at their servicing IACO or central processing facility (CPF). If a DOD ID cardholder has a manually produced card, he or she must obtain a machine-produced, bar-coded DOD ID card according to appropriate military regulations and personnel systems.

(b) Requesting an installation pass. Persons who do not have an authorized DOD ID card and require recurring unescorted access to U.S. Forces-controlled installations in Europe must request an installation pass. The installation pass may be issued only after the proper documentation has been submitted to the servicing IACO and the individual's DFMD has been provided.

(2) Carry their DOD ID card or installation pass on them while in a duty status or when on a U.S. Forces installation. On request, they will present their DOD ID card or installation pass to military law-enforcement personnel or guards. Refusal to present their DOD ID card or installation pass is a basis for immediately surrendering the card or pass and may be grounds for further administrative or punitive action.

(3) Immediately report a lost or stolen DOD ID card or installation pass to the local military police (MP) office.

(4) Inform the sponsoring organization of any change to the official relationship that served as the basis for access.

(5) 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.

(6) Register their POVs as part of the installation-pass application process if they plan to use a POV to enter U.S. Forces-controlled installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

6. POLICY

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

7. EXCEPTIONS TO POLICY

a. The USAREUR Provost Marshal (PM) may approve ETPs for up to 1 year.

b. Persons requesting an exception to any policy or procedure in this regulation must send their request through appropriate command channels to the OPM at e-mail: *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@mail.mil*.

c. USAG commanders may approve local ETPs where authorized to do so in this regulation.

d. ETPs that are embedded in the IACS software application may be administered locally by USAG DESs and do not require OPM approval. The OPM periodically audits and reviews software ETPs.

SECTION II
INSTALLATION ACCESS

8. ACCESS REQUIREMENTS

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

(1) They possess a valid DOD ID card that is registered in the IACS.

(2) They possess a valid regular or temporary U.S. Forces in Europe installation pass.

(a) Temporary installation passes have a red background in the title block to distinguish them from regular installation passes, which have a green background. Figure 1 shows samples of both passes.

Figure 1. Sample Temporary and Regular U.S. Forces in Europe Installation Passes

(b) Although these installation passes are similar in appearance, the restrictions associated with each are different. Differences between the temporary installation pass and the regular installation pass include the following:

1. A temporary installation pass is valid for up to 90 days and requires a Good Conduct Certificate (GCC) or an equivalent certificate resulting from a background check showing no adverse results.

2. A regular installation pass is valid for up to 5 years, depending on the category, and requires a GCC or an equivalent certificate and the completion of an HN background check, if available, with no adverse results (for example, the LNSP background check in Germany).

NOTE: Results of background checks that uncover adverse information must be forwarded to the sponsoring organization and the host USAG for adjudication. USAG and other commanders as well as security personnel will strictly control the results of security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander for action. Paragraph 28a(5)(c) provides additional guidance.

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

(a) Passport.

(b) National ID card issued by the country of citizenship (for example, the *Personalausweis* in Germany, the *Identiteitskaart* or *carte d'identité* (glossary) in Belgium, the *carta d'identità* (glossary) in Italy).

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

(d) HN military ID card.

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

(4) They are on an approved access roster and present one of the documents listed in subparagraphs (3)(a) through (e) above as well as the results of the background check if a background check is required.

NOTE: There may be situations when 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 USAG policy and approved by the USAG commander. In these situations, the policy in paragraph 7 still applies.

b. 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 installation 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, USAG commanders may approve ETPs for their USAG on a case-by-case basis (for example, for visiting immediate Family members). Persons with travel documents who have previously been issued an installation pass are grandfathered and may continue to use their installation pass for access until it expires. USAG commanders are the approving authorities for renewing those installation passes.

c. Individuals issued an *Ersatz-Personalausweis* (a replacement German national ID card) by the German Government are ineligible for a U.S. Forces in Europe 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 will deny access, contact the MP Desk, and provide details of the encounter. The USAG DES 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.

d. 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 USAG commander approval for USAG-wide access (that is, approval to be issued a U.S. Forces in Europe installation pass or a visitor paper pass) and USAG commander and USAREUR PM approval for Army-in-Europe-wide access. These individuals cannot be placed on an access roster. The sponsor will send a request for installation access through the USAG IACO to the responsible security office for preparation of a recommendation to the USAG commander. USAREUR guidance follows the U.S. Department of State requirement for an additional screening of citizens from identified countries before those 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).

e. Paragraph 38 prescribes policy for emergency-vehicle access. Paragraph 39 prescribes policy for special-vehicle access.

f. USAG commanders and Italian base 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, commanders may determine that additional documents (for example, a special pass) are required to gain access to their installation. Commanders are not authorized, however, to use these alternative access documents in place of DOD ID cards or U.S. Forces in Europe installation passes (regular or temporary).

SECTION III
INSTALLATION ACCESS CONTROL SYSTEM

9. DOD ID CARDS

a. IACS Registration. DOD ID cardholders stationed in Europe (on orders) must be registered in the IACS. In addition, the following individuals may be required to register in the IACS depending on their category:

(1) Reserve component (RC) DOD CAC ID cardholders (including dependents) who live and perform military duty within the USAREUR area of responsibility. These individuals will register as follows:

(a) RC DOD CAC ID cardholders with independent NATO SOFA status through other civilian employment will register in the IACS under either their civilian or military DOD ID card by providing proof of NATO SOFA status.

(b) RC DOD CAC ID cardholders without independent NATO SOFA status must provide a letter from their unit of assignment identifying them as a member of the unit and certifying that they have complied with HN residency requirements.

(2) RC DOD CAC ID cardholders who enter and leave the EU for the purpose of battle-assembly weekends (without independent NATO SOFA status, a visa, or residence permit). For these individuals, the individual's unit of assignment must provide the IACO documentation of the current-year battle-assembly and annual training schedules. Registration will be activated only during scheduled duty days, limited to 90 days total in a calendar year, and archived on nonduty days.

(3) DOD ID cardholders (for example, CAC holders) who are on TDY (on orders) in Europe for more than 72 hours. These individuals will be registered in the IACS for the duration of their TDY. This includes General Schedule (GS) employees with a blue-stripe CAC (for example, an instructor from the Defense Logistics Agency (DLA) teaching a language course).

(4) DOD ID cardholders (for example, active-duty military personnel, RC personnel, civilian personnel, military retirees and their dependents) who are visiting Europe. These individuals may be registered in the IACS for the duration of their visit, up to 90 days, or until the date specified by the HN visa.

(5) Military retirees (DD Form 2 (RES RET)) living in the EU. These individuals may be registered in the IACS for up to 5 years if they have a valid resident permit from an EU country.

(6) DOD civilian retirees who hold a civilian-retiree CAC. These individuals may be registered in the IACS for the USAG that is closest to where they physically reside if approved by the USAG commander or, in Italy, the base commander. DOD civilian retirees have no status under the NATO SOFA and are in Europe as residents or visitors with no on-base privileges. Commander approval memorandums must be on file at the responsible IACO and the OPM and will expire on change of command. Visitors may be registered in the IACS for the duration of their visit, up to 90 days, or until the date specified on the HN visa. DOD civilian retirees with a valid residence permit from an EU member country (*Aufenthaltstitel* in Germany) may be registered in the IACS for up to 2 years. USAG commanders may also approve U.S. Forces in Europe installation passes for spouses of retirees under the *Other* category (para 27). If approved for registration in the IACS, civilian-retiree CACs will be registered with the following privileges and restrictions:

(a) Days and Times Access is Authorized: 24 hours, 7 days a week.

(b) FPCON Restriction: Bravo.

(c) Visitor-Sponsor Privileges: Not authorized.

(7) DOD ID cardholders (including minors) who are EU citizens but are not command-sponsored. These individuals may be registered in the IACS for the duration of their stay or until the expiration date of their ID card, whichever is earlier.

(8) Contractor personnel who hold a CAC with a green stripe and the words IDENTIFICATION AND PRIVILEGES CARD on the bottom and who present documentation confirming their NATO SOFA status as contractors in the HN. These individuals will be registered in the IACS up to the expiration date of the CAC without an AE Form 190-16A.

(9) Contractor personnel who hold a CAC with a green stripe and only the words IDENTIFICATION CARD on the bottom. These individuals are U.S. contractor personnel without NATO SOFA status, logistic support, and privileges. They will be registered in the IACS as approved by AE Form 190-16A in accordance with paragraph 12. AE Form 190-16F may be used by the sponsor to register four or more individuals working under the same contract for the same event at the same location (for example, Exercise Austere Challenge, Exercise Combined Endeavor).

(10) Non-U.S. citizens who have been issued a CAC with a blue stripe.

(a) These individuals are required to register their CAC in the IACS in one of the following IACS categories:

1. Contractor (Resident of European Union (EU) or NATO-Member Country) (para 11).

2. Non-U.S. Military Member (para 18).

3. Local National Employee (para 19).

4. NATO Member (para 21).

(b) An installation pass will not be issued in those cases. The sponsor will use AE Form 190-16A to identify the required privileges and restrictions for installation access as defined in the respective category.

NOTE: Individuals who have multiple DOD ID cards (for example, a military retiree who is also a DA civilian employee or a contractor with NATO SOFA status in the HN) must choose which DOD ID card they want to use for IACS registration and then use that card to gain access to installations.

b. Restrictions. Unless imposed by a USAG commander or specified on AE Form 190-16A or AE Form 190-16F, no restrictions apply to the number of installations DOD ID cardholders may enter, the times they may enter, or FPCONs under which they may enter.

c. Visitor-Sponsor Privileges. DOD ID cardholders who are 18 years old or older may sponsor no more than four persons and their vehicles. USAG commanders and Italian base commanders may restrict or entirely deny this privilege.

d. Registering Minors. Minors must be registered in the IACS in the presence of a parent or legal guardian no later than 30 days after their 10th birthday.

10. ISSUANCE OF INSTALLATION PASSES AND REGISTRATION OF BLUE- AND GREEN-STRIPE COMMON ACCESS CARDS

Individuals who do not qualify for a CAC will be issued a U.S. Forces in Europe installation pass in one of the categories in subparagraphs a through q below. Individuals issued a blue-stripe CAC or a green-stripe contractor CAC will have their CAC registered in the IACS in the appropriate category based on AE Form 190-16A or AE Form 190-16F.

a. Contractor (Resident of European Union (EU) or NATO-Member Country) (para 11).

b. Contractor (U.S. Citizen Working for a U.S. Company Based in the United States) (para 12).

c. Delivery Personnel (Recurring Deliveries or Similar Services Not Associated With a Government Contract) (para 13).

d. Department of State and U.S. Embassy Personnel (para 14).

e. Foreign Student (Marshall Center) (para 15).

f. Gate Guard (para 16).

g. Host-Nation Government Official (para 17).

h. Non-U.S. Military Member (para 18).

i. Local National Employee (para 19).

j. Member of Private Organization (para 20).

k. NATO Member (para 21).

l. Official Guest (para 22).

m. Personal-Service Employee (para 23).

n. Vendor (Providing Merchandise or Services Not Associated With a Government Contract) (para 24).

o. Family Member (Immediate Family Member Living in Europe) (para 25).

p. Family Member (Family Member not Included in the Category Defined in Para 25) (para 26).

q. Other (para 27).

11. CONTRACTOR (RESIDENT OF EUROPEAN UNION (EU) OR NATO-MEMBER COUNTRY)

a. Definition: An individual without NATO SOFA status who lives in the EU or a NATO-member country and is contracted to work for DOD in Europe. Contractors who are trying to establish a contract with DOD may be granted access only through an individual who has visitor-sponsor privileges or through access-roster procedures.

b. Types of Passes Authorized:

(1) Temporary Installation Pass: Authorized after all required background checks have been completed and, for individuals in Germany, an LNSP screening has been initiated.

(2) Regular Installation Pass: Authorized after all background checks have been completed and returned with no entries.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for the length of the contract or up to 90 days, whichever is less.

(2) Regular Installation Pass: Valid for the length of the contract, up to 2 years, or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earliest.

d. Sponsors:

(1) Individuals appointed in writing as KOs, contracting officer's representatives (CORs), alternate contracting officer's representatives (ACORs), or site contracting officer's representatives (SCORs). If a KO, COR, ACOR, or SCOR is not available to perform the sponsor function (for example, if based in CONUS), he or she may appoint in writing an individual assigned to the USAREUR AOR as his or her USAREUR 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 Financial Management Support Center sponsors Community Bank contractors).

NOTE: All appointment letters will be on file on the USAREUR IACS portal.

e. Background Checks:

(1) GCC: Required before a temporary or regular installation pass may be issued.

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

f. Residence and Work Permits: Required for non-EEA citizens. (The USAREUR IACS SharePoint site provides current guidance.)

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

g. Installations a Passholder May Enter: Limited to the minimum number required for a contractor to perform his or her duties according to the contract performance work statement (PWS). A copy of the applicable portion of the PWS must be submitted with the application package. A vague or incomplete PWS limits an applicant's access to a single USAG until the PWS is revised.

h. Days and Times Access is Authorized: As specified in the PWS. A vague or incomplete PWS limits an applicant's access to Monday through Friday, 0800–1700 hours, until the PWS is revised.

i. Visitor-Sponsor Privileges:

(1) Visitor-sponsor privileges normally are not granted to contractors. USAG commanders or their designated appointees may approve visitor-sponsor privileges based on the justification provided on AE Form 190-16A as supported by the PWS.

(2) Visitor-sponsor privileges are not authorized at FPCON Delta.

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

(4) Visitor-sponsor privileges are not authorized for temporary-installation-pass holders.

j. FPCON Restrictions:

(1) Temporary-installation-pass holders: Bravo.

(2) Regular-installation-pass holders identified as—

(a) Nonessential personnel: Bravo.

(b) Essential personnel: Charlie.

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

12. CONTRACTOR (U.S. CITIZEN WORKING FOR A U.S. COMPANY BASED IN THE UNITED STATES)

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 for DOD in Europe temporarily.

b. Types of Passes Authorized:

(1) Temporary Installation Pass: Authorized up to 90 days in accordance with the required documentation.

(2) Regular Installation Pass: Authorized in accordance with the required documentation.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for the length of the visit or up to 90 days, whichever is less. For visits to Germany, a "fax-back" (note below) form is required before obtaining a temporary pass. AE Regulation 715-9 provides procedures for the fax-back process. For other countries, the sponsor is responsible for ensuring that all required country documents are completed before obtaining a temporary pass.

NOTE: "Fax-back" 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 Directorate, Office of the Deputy Chief of Staff, G1, HQ USAREUR (*http://www.eur.army.mil/g1/content/CPD/docper.html*).

(2) Regular Installation Pass: Valid for the length of the visit or up to 1 year, whichever is shorter. For work-related visits to Germany, depending on the situation, a fax-back form or an *Aufenthaltstitel* may be required before obtaining a regular installation pass (para 28a(6)). For example, a contractor who travels to Germany once a month or once a quarter and stays for 2 weeks must send a completed fax-back form to the appropriate IACO before arriving in Germany to activate the installation pass. The pass will be inactivated after the contractor departs. For other countries, the sponsor is responsible for ensuring all required country documents are completed before the contractor will obtain a regular installation pass.

d. Sponsors: Individuals appointed in writing as KOs, CORs, ACORs, or SCORs. If a KO, COR, ACOR, or SCOR is not available to perform the sponsor function (for example, if based in CONUS), he or she may appoint in writing an individual assigned to the USAREUR AOR as his or her USAREUR representative for sponsoring installation access. In Germany and Italy, the sponsor must ensure compliance with DOCPER policy (AE Reg 715-9).

e. Background Checks: A U.S. security check is required before a temporary or regular installation pass may be issued.

f. Residence and Work Permits: Depending on the HN, residence and work permits may be required. The DOCPER website at *http://www.eur.army.mil/g1/content/CPD/docper.html* and AE Regulation 715-9 provide further guidance.

g. Installations a Passholder May Enter: Limited to the minimum required for a contractor to perform his or her duties according to the PWS. A vague or incomplete PWS limits an applicant's access to a single USAG until the PWS is revised.

h. Days and Times Access Is Authorized: As specified in the PWS. A vague or incomplete PWS limits an applicant's access to Monday through Friday, 0800–1700 hours, until the PWS is revised.

i. Visitor-Sponsor Privileges:

(1) Visitor-sponsor privileges normally are not granted to contractors. USAG commanders or their designated appointees may approve visitor-sponsor privileges based on the justification provided on AE Form 190-16A as supported by the PWS.

(2) Visitor-sponsor privileges are not authorized at FPCON Delta.

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

(4) Visitor-sponsor privileges are not authorized for temporary-installation-pass holders.

j. FPCON Restrictions:

(1) Temporary-installation-pass holders: Bravo.

(2) Regular-installation-pass holders identified as—

(a) Nonessential personnel: Bravo.

(b) Essential personnel: Charlie.

13. DELIVERY PERSONNEL (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 perform similar services related to their employment (for example, pizza delivery personnel, taxi drivers).

b. Type of Pass Authorized: Regular installation pass. A regular installation pass is authorized after all background checks (including the LNSP screening in Germany) have been completed and returned with no entries.

c. Length of Time the Pass is Valid: Valid up to 2 years or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earlier.

d. Sponsor: The USAG within which deliveries are made or services are performed.

e. Background Checks:

(1) GCC: Required before a regular installation pass may be issued.

(2) U.S. Security Check: Required for U.S. citizens before a regular installation 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 screening must be completed and returned with no entries before a regular installation pass may be issued.

f. Residence and Work Permits: Required for non-EEA-country citizens. (The USAREUR IACS SharePoint site provides current guidance.)

g. Installations a Passholder May Enter: Limited to installations within the sponsoring USAG.

h. Days and Times Access is Authorized: As specified by the sponsor.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

14. DEPARTMENT OF STATE AND U.S. EMBASSY PERSONNEL

a. Definition: 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 AE Regulation 600-700.

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for the length of the individual's tour (not to exceed 5 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.

d. Sponsors: United States Missions in countries in the USEUCOM and USAFRICOM areas of operation. The United States Mission in the country in which an individual is stationed will send DD Forms 577 designating sponsoring officials by e-mail to the OPM at *usarmy.wiesbaden.usareur.list.g34-opm-iacs-operations@mail.mil*. Individuals in this category may obtain their installation pass at any USAREUR IACO. Since these individuals are located throughout Europe and Africa, their first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the USAG IACO to obtain an installation pass according to paragraph 28.

e. Background Checks: Not required.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: No restrictions.

h. Days and Times Access is Authorized: No restrictions.

i. Visitor-Sponsor Privileges: Authorized.

j. FPCON Restrictions: None.

15. FOREIGN STUDENT (MARSHALL CENTER)

a. Definition: A foreign military student assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany.

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for up to 2 years, the length of a student's tour, or until the expiration date of the supporting document that was used to obtain the installation pass (for example, military ID card), whichever is earliest.

d. Sponsor: The Marshall Center.

e. Background Checks: Not required.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to installations in the Garmisch Military Community.

h. Days and Times Access is Authorized: No restrictions.

i. Visitor-Sponsor Privileges: Authorized.

j. FPCON Restrictions: None.

16. GATE GUARD

a. Definition: A contract security gate guard in a position responsible for controlling access to an installation.

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for up to 2 years or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earlier.

d. Sponsor: The COR, ACOR, or the USAG SCOR.

e. Background Checks: As required under the conditions of employment. Either the Emergency Services Branch, Office of the Assistant Chief of Staff, G3, IMCOM-Europe, or the responsible USAG DES will verify that all required background checks have been completed.

f. Residence and Work Permits: Residence and work permits are required if the applicant is not an EEA-country citizen (para 28a(6)). Residence and work permits will be verified by the OPM as a condition of employment.

g. Installations a Passholder May Enter: Limited to installations within the USAG to which a guard is assigned. If assigned to more than one USAG (for example, dog handlers, area supervisors), the guard will be placed in the *Contractor (Resident of European Union (EU) or NATO-Member Country)* category (para 11).

h. Days and Times Access is Authorized: No restrictions.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restrictions: None.

17. HOST-NATION GOVERNMENT OFFICIAL

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), or an employee of an HN government office.

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for up to 2 years or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earlier.

d. Sponsor: Depending on the type of official guest. In most cases, the USAG to which access is required will sponsor HN government officials.

e. Background Checks: Not required.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to the minimum required for the HN government official to conduct official business.

h. Days and Times Access is Authorized: As authorized by the sponsoring organization.

i. Visitor-Sponsor Privileges: Not authorized unless justified by the sponsoring organization. If authorized, visitor-sponsor privileges are granted "for official business only."

j. FPCON Restriction: Charlie.

18. NON-U.S. MILITARY MEMBER

a. Definition: A military member of the armed forces of a foreign nation and his or her accompanying Family members (children up to the age of 21) who are stationed on a U.S. Forces-controlled installation (for example, a foreign liaison officer assigned to HQ USAREUR). This category should not be confused with the *NATO Member* category (para 21).

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for up to 2 years, for the length of the non-U.S. military member's tour, or until the expiration date of the supporting document that was used to obtain the installation pass (for example, a military ID card), whichever is earlier.

d. Sponsor: The non-U.S. military member's sponsoring organization. If no sponsoring organization exists, the USAG within which the individual is stationed will perform sponsor responsibilities.

e. Background Checks: Not required.

f. Residence and Work Permits: Normally not required.

g. Installations a Passholder May Enter: Limited to the minimum required based on the non-U.S. military member's duties.

h. Days and Times Access is Authorized: As specified by the sponsor.

i. Visitor-Sponsor Privileges: Authorized**.**

j. FPCON Restrictions: None.

19. LOCAL NATIONAL EMPLOYEE

a. Definition. 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. Furthermore, they apply to HN interns performing an internship with an Army in Europe organization.

b. Types of Passes Authorized:

(1) Temporary Installation Pass: Authorized after all required background checks have been completed and, for LN employees in Germany, an LNSP screening has been initiated. The temporary installation pass will be used only until a regular installation pass is authorized.

(2) Regular Installation Pass: Authorized after all background checks (e below) have been completed and returned with no entries.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for up to 90 days.

(2) Regular Installation Pass—

(a) Without Visitor-Sponsor Privileges: Valid for up to 5 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) With Visitor-Sponsor Privileges: Valid for up to 3 years.

d. Sponsor: The organization for which the LN employee will work.

e. Background Checks:

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

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

(4) Exceptions to the Requirement for Background Checks:

(a) LN employees in Germany hired by a U.S. Consulate may use the memorandum signed by the Consulate's regional security officer (RSO) that certifies that the individual has a valid security clearance or certification instead of providing a GCC or completing the LNSP requirement.

(b) LN employees with a current U.S. or NATO Secret or higher clearance may use that clearance instead of providing a GCC or completing the HN background check.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to the minimum number required for the LN employee to perform his or her duties.

h. Days and Times Access is Authorized: Limited to the LN employee's work-schedule requirements as determined by the sponsor.

i. Visitor-Sponsor Privileges: Temporary-installation-pass holders are not authorized visitor-sponsor privileges. Regular-installation-pass holders and CAC holders are not authorized visitor-sponsor privileges unless justified by the sponsoring organization. If authorized, visitor-sponsor privileges will be granted up to the expiration of the installation pass or CAC. Visitor-sponsor privileges for installation-pass holders are not authorized during FPCON Charlie and Delta.

j. FPCON Restrictions:

(1) Temporary-installation-pass holders: Bravo.

(2) Regular-installation-pass holders identified as—

(a) Nonessential personnel: Bravo.

(b) Essential personnel: Charlie.

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

20. MEMBER OF PRIVATE ORGANIZATION

a. Definition: 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.

b. Type of Pass Authorized: Regular installation pass. A regular installation pass is authorized after all background checks (including the LNSP screening in Germany (e(3) below)) have been completed and returned with no entries.

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

d. Sponsor: The USAG at which PO functions are performed.

e. Background Checks:

(1) GCC: Required before a regular installation pass may be issued.

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 regular installation pass may be issued.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to installations within the sponsoring USAG.

h. Days and Times Access is Authorized: As authorized by the sponsoring USAG.

i. Visitor-Sponsor Privileges. Not authorized.

j. FPCON Restriction: Bravo.

21. NATO MEMBER

a. Definition: A NATO military member, civilian employee, and their dependent Family members (up to age 23). This category is designed for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military) who meet the requirements in AE Regulation 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, USAFE). This category should not be confused with the *Non-U.S. Military Member* category (para 18).

b. Type of Pass Authorized: Regular installation pass.

c. Length of Time the Pass is Valid: Valid for up to 2 years or for the length of the member's tour, whichever is earlier.

d. Sponsors:

(1) NATO Members Assigned to an International Military Headquarters, Activity, or Special Mission in Germany, or to a U.S. Military Headquarters: The parent organization will sponsor individuals in this category.

(2) Active-Duty Belgian, British, Canadian, Dutch, and French Military ("Sending States"): The security office of the Sending State will sponsor individuals in this category. The Sending State will send DD Forms 577 designating sponsoring officials by e-mail to the USAREUR OPM at *iacs3@eur.army.mil*. The OPM will post DD Forms 577 to the IACS portal where the forms will be available to all IACOs. Individuals in this category may obtain an installation pass at any IACO. Since these individuals are stationed throughout the European theater, the first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the responsible IACO to obtain an installation pass in accordance with paragraph 28.

(3) British and French Consular and Diplomatic Personnel Stationed in Germany: The U.S. Mission, Germany (Department of State), will sponsor individuals in this category. The U.S. Mission, Germany, will send DD Forms 577 designating sponsoring officials by e-mail to the USAREUR OPM at *iacs3@eur.army.mil*. The OPM will post DD Forms 577 to the IACS portal where the forms will be available to all IACOs. Individuals in this category may obtain their installation pass at any IACO. The first visit of British and French consular and diplomatic personnel to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the responsible IACO to obtain an installation pass in accordance with paragraph 28.

e. Background Checks: Not required.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to U.S. Forces installations in the country of assignment.

h. Days and Times Access is Authorized: No restrictions.

i. Visitor-Sponsor Privileges: Authorized.

j. FPCON Restrictions: None.

22. OFFICIAL GUEST

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. 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) Volunteers (for example, Family and morale, welfare, and recreation (FMWR) volunteers).

(3) Interns participating in exchange programs.

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

(5) New hires who cannot immediately receive a CAC (for example, LN employees).

(6) Dependents of same-sex couples (DOD military members, civilians, contractors with technical-expert-status accreditation). Sponsors will review, but not keep, documentation verifying the relationship (for example, marriage license, domestic partnership license, civil union license). If the documentation is not available in English, it must be translated.

(7) Individuals approved on a Family Care Plan (DA Form 5305 or Air Force Form 357).

NOTE: The examples in (1) through (7) above are not all-inclusive. Sponsoring organizations will not use this category when an applicant meets the definition of another, more restrictive category.

b. Types of Passes Authorized:

(1) Temporary installation pass.

(2) Regular installation pass.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for up to 90 days.

(2) Regular Installation Pass: Valid for up to 2 years, until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), or until the expiration date of the agreement or supporting memorandum, whichever is earliest.

d. Sponsor: Depending on the type of official guest. In most cases, the USAG to which access is required will sponsor individuals in this category and perform sponsor responsibilities.

e. Background Checks:

(1) GCC: Required for HN citizens and residents before a temporary or regular installation pass may be issued.

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

(4) Exceptions to the Requirement for Background Checks: Because of the broad nature of this category, the responsible USAG commander may grant ETPs on a case-by-case basis. In addition, background checks are not required for individuals with member-of-household status and dependents of same-sex couples.

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

g. Installations a Passholder May Enter: Limited to the minimum number the guest requires to enter based on his or her official relationship with the U.S. Government.

h. Days and Times Access is Authorized: As specified by the sponsoring organization.

i. Visitor-Sponsor Privileges: With the exception of individuals with member-of-household status and dependents of same-sex couples, individuals in this category are not authorized visitor-sponsor privileges unless approved by the USAG commander.

j. FPCON Restrictions:

(1) Temporary-installation-pass holders: Bravo.

(2) Regular-installation-pass holders identified as—

(a) Nonessential personnel: Bravo.

(b) Essential personnel: Charlie.

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

23. PERSONAL-SERVICE EMPLOYEE

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

b. Types of Passes Authorized:

(1) Temporary Installation Pass: Authorized after all required background checks have been completed and returned with no entries and the LNSP screening in Germany has been initiated.

(2) Regular Installation Pass: Authorized after all background checks including the LNSP screening in Germany have been completed and returned with no entries.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for the length of service or up to 90 days, whichever is earlier.

(2) Regular Installation Pass: Valid for the length of service, for 2 years, or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earliest.

d. Sponsor: The USAG within which the requester resides.

e. Background Checks.

(1) GCC: Required before a temporary or regular installation pass may be issued.

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

f. Residence and Work Permits: May be required for non-EEA citizens (para 28a(6)).

g. Installations a Passholder May Enter: Limited to the installation within the USAG where the requester resides.

h. Days and Times Access is Authorized: As specified by the requester or sponsor.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

24. VENDOR (PROVIDING MERCHANDISE OR SERVICES NOT ASSOCIATED WITH A GOVERNMENT CONTRACT)

a. Definition: An individual who is authorized to offer insurances, 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 is not associated with a Government contract. Vendors providing merchandise or services under a Government contract (for example, Army and Air Force Exchange Service (AAFES), Defense Commissary Agency, FMWR, nonappropriated fund non-personal-services contractors and concessionaires) are contractors and will not be placed in this category.

b. Type of Pass Authorized: Regular installation pass. A regular installation pass is authorized after all background checks including the LNSP screening in Germany (e(3) below) have been completed and returned with no entries.

c. Length of Time the Pass is Valid: Up to 2 years, until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), or until the expiration date of the vendor's permit, whichever is earliest.

d. Sponsor: The USAG within which the vendor conducts business. When access is required for more than one USAG, the applicant must be sponsored by AAFES-Eur; the Defense Commissary Agency, Europe; or IMCOM-Europe. This sponsoring authority may not be delegated to subordinate organizations.

e. Background Checks:

(1) GCC: Required before a regular installation pass may be issued.

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

(3) HN Background Check: Required, if available, for both non-U.S. citizens and 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 regular installation pass may be issued.

f. Residence and Work Permits: May be required for non-HN citizens (para 28a(6)).

g. Installations a Passholder May Enter: Depending on the level of the sponsoring organization (d above).

h. Days and Times Access is Authorized: As specified by the sponsor.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

25. FAMILY MEMBER (IMMEDIATE FAMILY MEMBER LIVING IN EUROPE)

a. Definition: A Family member of the requester, age 10 or older, who legally resides within the EEA. For the purpose of this regulation, 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. Type of Pass Authorized: Regular installation pass. A regular installation pass is authorized only if the requester resides on a controlled-access installation (glossary). If the requester resides off a controlled-access installation, the USAG commander may approve an installation pass based on the extenuating circumstances presented by the requester.

c. Length of Time the Pass is Valid: Up to 2 years or until the expiration date of the supporting document that was used to obtain the installation pass (for example, passport), whichever is earlier.

d. Sponsor: The requester.

e. Background Checks:

(1) GCC: Required before a regular installation pass may be issued.

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

NOTE: Background checks are not required for minors under the age of 18.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Limited to installations within the USAG where the requester resides. The USAG may impose further restrictions. The holder of a valid Family member installation pass, when accompanied by a DOD ID cardholder, will be authorized to temporarily access areas that exceed the assigned access level, when required.

h. Days and Times Access is Authorized: As specified by the sponsor.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

26. FAMILY MEMBER (FAMILY MEMBER NOT INCLUDED IN THE CATEGORY DEFINED IN PARA 25)

a. Definition: A Family member of the requester, age 10 or older, who does not reside within the EEA and is not included in the category in paragraph 25.

b. Type of Pass Authorized: Regular installation pass. A regular installation pass is authorized only if the requester resides on a controlled-access installation. If the requester resides off a controlled-access installation, the USAG commander may approve an installation pass based on the extenuating circumstances presented by the requester.

c. Length of Time the Pass is Valid: For the length of the visit or up to 90 days, whichever is less, according to Schengen visa requirements for non-Schengen-zone citizens.

d. Sponsor: The requester.

e. Background Checks:

(1) GCC: Required before a regular installation pass may be issued.

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

NOTE: Background checks not required for minors under the age of 18.

f. Residence and Work Permits: Not required. A visa, however, may be required.

g. Installations a Passholder May Enter: Limited to installations within the USAG where the requester resides. The holder of a valid Family member installation pass, when accompanied by a DOD ID cardholder, will be authorized to temporarily access areas that exceed the assigned access level, when required.

h. Restrictions on Days and Times Access is Authorized: As specified by the sponsor.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

27. OTHER

a. Definition: Individuals who require recurring and unescorted access, but who do not meet the definition of any other person category. USAGs will review the access requirements for each applicant and evaluate the extenuating circumstances. An example for this category would be a spouse or dependent who transports an installation-pass holder who has either a permanent physical handicap or is temporarily disabled (for example, broken leg, recent surgery).

NOTE: In Germany, parents or guardians of DOD dependents who have an approved AE Form 550-175K are eligible for a pass in this category.

b. Types of Passes Authorized:

(1) Temporary installation pass.

(2) Regular installation pass.

c. Length of Time the Passes are Valid:

(1) Temporary Installation Pass: Valid for up to 90 days.

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

d. Sponsor: The USAG to which access is required.

e. Background Checks:

(1) GCC: Required before a temporary or regular installation pass may be issued.

(2) U.S. Security Check: Required for U.S. citizens before a temporary or regular installation 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 initiated before a temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

f. Residence and Work Permits: Not required.

g. Installations a Passholder May Enter: Installations within the sponsoring USAG.

h. Days and Times Access is Authorized: As specified by the sponsoring USAG.

i. Visitor-Sponsor Privileges: Not authorized.

j. FPCON Restriction: Bravo.

SECTION IV
INSTALLATION PASS

28. APPLICATION PROCESS

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

(1) Sponsoring Organization. The sponsoring organization will designate individuals within its organization to carry out sponsoring-organization responsibilities. The sponsoring organization for each applicant is based on the applicant's category (paras 11 through 27). For example, USAGs will serve as sponsoring organizations for some applicants; hiring organizations will serve as sponsoring organizations for other applicants.

(2) Sponsoring Official.

(a) The sponsoring official is key to the integrity of the IACP.

(b) A lieutenant colonel or a GS-13 civilian in the chain of command of an organization that sponsors installation-pass applicants will designate sponsoring officials in writing using DD Form 577. If a sponsoring organization does not have this military or civilian pay-grade structure, the local senior manager or deputy of the organization is authorized to designate sponsoring officials using DD Form 577.

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

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

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

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

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

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

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

1. Supervisors in the grade of lieutenant, sergeant first class, chief warrant officer 2, GS-9, NF-3, C6A, or above are authorized to sponsor individuals for single-installation access only.

2. Supervisors in the grade of captain, first sergeant or master sergeant, chief warrant officer 3, GS-11, NF-4, C7, or above are authorized to sponsor individuals for USAG-wide access.

3. Supervisors in the grade of lieutenant colonel, GS-13, NF-5, C8, or above are authorized to sponsor individuals for USAREUR-wide access. Paragraph 11 provides additional restrictions for applicants in the *Contractor (Resident of European Union (EU) or NATO-Member Country)* category.

4. There are no grade restrictions for KOs, CORs, ACORs, SCORs, or appointed contractor representatives.

NOTE: USAGs in Belgium, Italy, and the Netherlands may use equivalent pay-grade structures for their LN employees.

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

(3) Category. An applicant's category will determine the type of installation pass that may be issued and the associated restrictions. Sponsoring officials will enter the category in block 7 of AE Form 190-16A, and IACS registrars will verify its correctness. Registration requirements and restrictions vary among the different categories.

(4) Type of Installation Pass Requested. Sponsors will request either a temporary or regular installation pass based on an applicant's category and the circumstances under which the applicant is applying.

(5) 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. Directive-Type Memorandum (DTM) 09-012 provides a detailed definition of fitness and the vetting process through which an individual's fitness is determined. Sponsoring organizations are responsible for initiating required background checks and ensuring background checks are completed. They should refer to the appropriate category (paras 11 through 27) to determine the background-check requirements for each applicant. IACS registrars are responsible for verifying that a background check has been completed or, where applicable, initiated. The types of background checks used for installation passes are as follows:

1. GCC. An applicant will obtain this certificate from his or her local registration office (for example, the *Meldebehörde* in Germany). A certified translation must be obtained for all GCCs that are not completed in English, German, or Italian. Certificates that are more than 12 months old may not be used. If an individual is unable to get a GCC in the current country of residence (for example, if he or she 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. The USAG DES will use all authorized databases that are available to vet an applicant (for example, MP databases, the Security Forces Management Information System (SFMIS), National Crime Information Center databases). Sponsoring officials will request U.S. security checks from their servicing MP station using AE Form 190-45D.

3. HN Background Check. An HN 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 AE Regulation 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. The LNSP screening must be initiated before a temporary installation pass may be issued. The screening must be completed and returned with no entries before a regular installation pass may be issued.

NOTE: LN employees who have been issued a DOD CAC (blue- or green-stripe) have already completed the required background checks.

a. In Germany, sponsoring officials will notify the IACO at which a temporary installation pass was issued either in person or by e-mail when the LNSP background check has been completed.

b. Once the HN background check has been completed (without entries), the applicant must return the temporary installation pass to the issuing IACO to obtain a regular installation pass.

(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 sponsoring organization and the responsible USAG. The USAG will use the commander's adjudication policy based on AD 2014-05 to coordinate with the sponsoring organization to determine whether the adverse information warrants denial of access privileges. If access to more than one USAG is requested and the USAG commander recommends approval, the IACS Program Office, OPM, will adjudicate on the applicant's installation-pass request. Adjudication packages submitted to the IACS Program Office must include the USAG commander's approval memorandum, AE Form 190-16A, LNSP screening results, a GCC, and any supporting memorandums from the applicant and his or her supervisor.

1. If a USAG denies an applicant an installation pass based on the adverse results of a background check, the applicant will not be placed on an access roster.

2. If, based on adverse information resulting from a background check, OPM denies an Army-in-Europe-wide installation pass to an applicant whose access request is supported by the USAG commander, the USAG commander may assume the potential risk and approve issuance of an installation pass for only his or her USAG.

(d) If an applicant is unable to obtain a background check, the USAG should review the situation and make a determination based on a risk assessment. USAGs 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 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 installation pass to have the expiration date coincide with the date on which the individual will have 12 months of residency in the HN.

(6) Residence and Work Permits. USAGs are required to follow HN guidance on residence and work permits. The OPM will post current HN guidance on the USAREUR IACS portal.

(7) Installations a Passholder May Enter. Specific justification is required for an individual to gain access to an installation. The individual's sponsoring official will—

(a) Ensure the application indicates the minimum number of installations within a USAG to which access is required, as provided by supporting documentation (for example, a contract PWS listing specific names of installations (for example, Clay Kaserne)).

(b) Provide specific detailed justification if recurring access to a USAFE installation is required. The air-base wing security official will review the justification and approve or disapprove access or ask for additional information.

NOTE: The responsible IACO will contact the USAFE air-base IACO POC to obtain approval for installation access for that air base. A USAFE IACO POC list is available under the Air Force button on the IACS SharePoint portal at *https://intranet.eur.army.mil/hq/opm/sea/iacs/SitePages/Home.aspx*.

(8) Days and Times Access is Authorized. An individual's sponsoring official must review the installation-access requirement and limit access to the minimum days and times access is required.

(9) Visitor-Sponsor Privileges. Applications must provide sufficient justification that clearly explains why an installation-pass holder requires visitor-sponsor privileges. Only USAG commanders and Italian base commanders or their designated representatives are authorized to review and approve requests for visitor-sponsor privileges.

(10) FPCON Restrictions. FPCON restrictions are based on an individual's category and function (nonessential, essential, first or emergency responder). The IACS prohibits access beyond the FPCON associated with a category (paras 11 through 27). 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.

(11) Vehicle Information. All individuals applying for an installation pass will register the POVs they use to enter a U.S. installation. Proof of POV ownership is not required for IACS registration.

(12) Installation Passes for Minors. Installation passes are required for minors no later than 30 days after their 10th birthday (for example, dependents of NATO members or U.S. consulate personnel).

b. Processing an Application.

(1) Sponsoring officials will complete AE Form 190-16A in English using U.S. standard measurements (app B) and digitally sign the form to sponsor an individual for a temporary or regular installation pass for the following reasons:

(a) To request a temporary or regular installation pass (first-time pass).

(b) To renew a pass that has expired or is about to expire.

(c) To replace a pass that was lost or stolen.

(d) To extend a temporary installation pass.

(e) To register or renew a blue-stripe CAC in the IACS.

(f) To register or renew a green-stripe CAC (ID card for U.S.-based contractors) in the IACS.

NOTE: Sponsors who do not have a CAC (for example, members of a U.S. consulate human-resources staff) may manually sign AE Form 190-16A.

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

(a) A copy of one of the following:

1. Passport.

2. 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).

NOTE: Applicants must bring their original passport or ID card to the IACO to validate their identity ((8) below).

(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.

NOTE: U.S. Department of State and NATO IDs as well as HN military, national police, and customs IDs (for example, *Dienstausweis* in Germany) may not be copied. Sponsoring officials may only view these documents.

(3) When an application is complete, the sponsoring official will send it by e-mail to the responsible IACO. The e-mail message must be sent encrypted.

(4) The IACO will verify that the e-mail 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 (for a temporary installation pass) or completed (for a regular installation pass).

(6) IACS registrars will review applications and supporting documents and reject any application that is not complete. IACS registrars 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 provide the applicant the required details for visiting the IACO and completing the application process. For first-time issue of an installation pass, the sponsor will either escort the applicant to the IACO or place him or her on an access roster (AE Form 190-16F).

(9) Before the IACS registrar will issue an installation pass to an applicant, the applicant must sign AE Form 190-16E and AE Form 190-16K. The IACS registrar will ensure that the applicant reads and understands the contents of the forms before the applicant signs them.

NOTE: If an applicant does not speak, read, or understand any of the HN languages, the sponsor is responsible for having someone available during the application process to provide translation services and ensure the applicant understands his or her responsibilities and the contents of the documents he or she is signing.

(10) The IACS registrar will electronically file the completed application packet in accordance with the OPM IACS Army Records Information Management System (ARIMS) memorandum for record.

29. APPLICATION PROCEDURES FOR APPLICANTS WITH A TEMPORARY INSTALLATION PASS

Sponsoring organizations are not required to submit a new application (AE Form 190-16A) for individuals who already have a temporary installation pass to obtain a permanent pass. Instead, the following procedures apply:

a. Sponsoring officials will notify the responsible IACO by e-mail about where the temporary installation pass was issued and, for LN employees in Germany, the date the LNSP screening was completed and a statement was provided confirming that the results included no adverse information. If adverse information was found, the notification must state that the host USAG and the sponsoring official have reviewed the results and determined that no adverse information exists that warrants denial of installation-access privileges. The notification must also include any changes to the data provided on AE Form 190-16A that have occurred since the temporary installation pass was issued.

b. After the IACO receives the notification, the applicant will return the temporary installation pass and obtain a regular installation pass. The IACO will file the notification with the original temporary-installation-pass application packet.

NOTE: The IACO will verify the sponsoring official's DD Form 577 before processing the application.

30. PROCEDURES FOR RENEWING AN INSTALLATION PASS

a. To renew an installation pass, sponsoring officials will submit a new application (AE Form 190-16A) to validate the information on the original application. Requests may be processed as early as 45 days before the expiration date of the current pass. IACOs may issue a renewal 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, TDY).

b. The following applies to background checks that are required when an applicant renews an installation pass:

(1) A new GCC is required if both of the following apply:

(a) A certificate is required based on the person's category.

(b) The previous certificate is more than 12 months old.

NOTE: Subparagraphs (1)(a) and (b) above do not apply to individuals in the *LN Employee* category (para 19).

(2) For U.S. citizens, a new U.S. security check is required if one was initially requested.

(3) Unless extraordinary circumstances exist, a new LNSP screening will not be required. Sponsoring officials will use the verification from the original LNSP screening.

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

d. Before issuing a new installation pass, IACOs will ensure applicants turn in their expiring or expired installation pass or AE Form 190-16B showing that access-control personnel confiscated an expired pass.

NOTE: Individuals in the *LN 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. These transfers are documented on the application for a new installation pass.

31. PROCEDURES FOR REPLACING A LOST OR STOLEN INSTALLATION PASS

If an installation pass is lost or stolen, the installation-pass holder must immediately report the loss or theft to the local MP station and IACO. The installation pass will be flagged in the IACS as lost or stolen. The sponsoring organization must submit a new application to the same IACO that issued the original installation pass. If requested by the sponsoring official in the application, the expiration date of the installation pass may be extended to show a full registration period authorized for that individual's category. With the exception of LN employees, a new GCC may be required if the current GCC is older than 12 months.

32. PROCEDURES FOR EXTENDING A TEMPORARY PASS

a. In Germany, IACOs may grant two 90-day extensions to a temporary installation pass when an LNSP screening was conducted, but the results have not yet been received. If the results of an LNSP screening reveal adverse information, another temporary installation pass will not be issued.

b. Background checks that reveal adverse information will be processed in accordance with paragraph 28a(5)(c).

33. UNSERVICEABLE PASSES

An unserviceable (glossary) installation pass may be exchanged one for one at the passholder's servicing IACO without action by the sponsoring organization. If the pass was confiscated by an MP official or access-control personnel, the receipt (AE Form 190-16B) will be used to obtain a new pass. The expiration date on the replacement pass will be the same as that on the original installation pass.

SECTION V
INSTALLATION ACCESS CONTROL OFFICE

34. GENERAL

a. Access control is a USAG commander's or Italian base commander's responsibility. USAGs and, in Italy, bases are the only organizations that are authorized to issue installation passes or to be equipped with IACS scanners.

b. USAGs will functionally align their IACOs under their DESs.

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

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

(2) Develop a system to reconcile with each sponsoring organization every 6 months to ensure the IACS database accurately shows the individuals the sponsoring organization has identified as current.

(3) Take the following actions to ensure that the security, accountability, and procurement of installation-pass material is maintained:

(a) Record the destruction of all installation passes on AE Form 190-16C and annotate the final disposition of passes in the IACS.

(b) Control and keep an adequate stock of passes, laminate, and ribbons at all times.

35. REGISTRATION PROCEDURES FOR IDENTI-KID

Parents and legal guardians with children under the age of 10 who do not have DOD ID cards may register their children in the IACS using Identi-Kid. Identi-Kid provides a way to collect a current photograph, fingerprints, vital statistics, and contact information. This information is used to help locate missing children. A parent or guardian in possession of a DOD ID card must be present to register a child.

SECTION VI
ACCESS PROCEDURES

36. ESCORTED-VISITOR PAPER PASS

The escorted-visitor paper pass (fig 2) provides short-term access (that is, up to 3 days unless further restricted by local policy) to USAREUR installations when an access roster and an installation pass are impractical or not authorized.

a. Visitor-Sponsor Privileges.

(1) DOD ID cardholders who are 18 years old or older and military spouses under the age of 18 have visitor-sponsor privileges. If this privilege has been suspended, the suspension will be documented in the IACS. Guards will check the IACS for visitor-sponsor privileges when an individual tries to use these privileges.

(2) Except for individuals in the *NATO Member*, *Non-U.S. Military Member*, and *Department of State and U.S. Embassy Personnel* categories, installation-pass holders are not granted visitor-sponsor privileges unless authorized by the sponsoring organization. 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) Temporary-installation-pass holders are not authorized visitor-sponsor privileges.

(2) DOD ID cardholders not registered in the IACS are not authorized visitor-sponsor privileges.

(3) Visitor sponsors are limited to sponsoring four individuals and their vehicles at any one time.

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

Figure 2. Sample Escorted-Visitor Paper Pass

(5) When visitor-sponsor privileges are abused or violate USAG policy, USAG commanders and Italian base commanders may revoke them. If revoked, they are revoked USAREUR- and USAFE-wide.

c. FPCON Restrictions. During FPCON Charlie, HN contractors and official guests are not authorized visitor-sponsor privileges. During FPCON Delta, only DOD ID cardholders are authorized visitor-sponsor privileges. Exceptions may be granted by USAG commanders for key and essential personnel (glossary).

d. 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 IACS passport and document scanner to validate the passport or personal ID and 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.

e. 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 his or her 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, 120 days for the second offense, and 1 year for the third offense. USAG commanders may provide additional restrictions and limitations per commander's policy letter.

f. Minors. Minors under the age of 10 do not require an escorted-visitor paper pass, but must be accompanied by a sponsored escorted-visitor paper-pass holder who is at least 18 years old.

g. Technical Difficulties. If the NIPR connection is unavailable or the printer is inoperable at the visitor gate, the gate will automatically revert to a sign-in process until the NIPR connection is restored or the printer is fixed or replaced. During the sign-in process, the sponsor and visitor information is manually recorded in the IACS computer at the ACP. Under these circumstances, sponsors are required to return to the ACP to sign out their visitors after their visit.

h. AE 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 AE Form 190-16E and sign the form or visitor log book before receiving their escorted-visitor paper pass.

NOTE: If an applicant does not speak, read, or understand any of the HN languages, the sponsor is responsible for ensuring that the applicant understands his or her responsibilities and the contents of the documents he or she is signing.

37. ACCESS ROSTERS

a. Access rosters are used to provide access to installations when issuing a visitor paper pass or an installation pass is impractical or not authorized.

b. Permanent access rosters are not authorized. Access rosters are temporary and will not be used to circumvent the installation-pass process. The maximum time an access roster may remain valid is 30 days.

c. Access rosters are used for events that are nonrecurring and not regularly scheduled, are generally site-specific, and must be coordinated in advance.

d. Access rosters may be used for contractors who have a current GCC (that is, issued within the past 12 months) and are identified as temporary hires (up to 30 days). Temporary hires are individuals who are not permanently employed working on a recurring and regular basis, but who are on call to substitute for a permanent employee.

e. Contractors with a current GCC may be placed on an access roster multiple times as long as their installation access is nonrecurring and not regularly scheduled (for example, a repair person requiring access to fix playground equipment).

f. Individuals with an adverse GCC or an LNSP screening that has not been adjudicated will not be placed on an access roster.

g. The following are examples of when access rosters should or should not be used:

(1) Example 1: An authorized DOD ID cardholder requires four meetings with several HN citizens (not associated with the U.S. Armed Forces) over a 3-week period to discuss a project. An access roster would be appropriate for the HN citizens because the meetings are not regularly scheduled, are site-specific, and are not scheduled beyond 30 days.

(2) Example 2: A sanctioned private organization (for example, dance club) meets every Wednesday evening at 1900. Several of the members are HN citizens. An access roster is not appropriate because the meetings are considered a recurring event. The participants must be signed in each week or be issued an installation pass based on the *Member of Private Organization* category (para 20).

(3) Example 3: The directorate of public works hires a contractor to perform construction work on an installation for 2 weeks. An access roster is appropriate because the contract is for only 2 weeks and is site-specific.

(4) Example 4: A DOD ID cardholder wants to host a surprise birthday party at a Family and morale, welfare, and recreation facility. The guest list includes 10 individuals who have no means of access. An access roster is appropriate because the party is a single event and site-specific.

h. The following policy applies to access rosters:

(1) Only DOD ID cardholders (including LN CAC holders with visitor-sponsor privileges) and NATO and non-U.S. military members with a CAC who are registered in the IACS may sign requests for an access roster (AE Form 190-16F). IACS registrars will check the IACS to ensure a requester is authorized to sign an access-roster request.

(2) Requests for an access roster (AE Form 190-16F) must be sent from official e-mail accounts (for example, accounts ending in .aafes.com, .eu.dodea.edu, .gov, .mil, .nato). All requests must be sent by encrypted e-mail. IACO officials will confirm receipt.

(3) To ensure IACS registrars have enough time to process access rosters, requests must be submitted no later than 3 workdays before the desired effective date of the roster.

(4) Access rosters must include the following information:

(a) The full name, nationality, date of birth, ID number (from one of the documents in paragraph 8a(3), which must be shown to the guard before access is granted), and the vehicle license-plate number, if applicable, for each individual.

(b) An effective date and an expiration date. (Access rosters may be valid no longer than 30 days.)

(c) The reason for the request, the location of the event or the work to be performed, and the ACPs to which the access roster applies.

(d) If an access roster is used to support a contractor or delivery service, the company's name and telephone number.

(e) If an access roster is used to support nonrecurring delivery services, the day and time for which delivery is scheduled (for example, 1 April 2017 from 0800 to 1200).

(5) If an access roster is used for contract workers or vendors (for example, construction crew, vendors for a community event such as a bazaar or a technology fair, contracted employees for a specific service such as conducting an inventory or for contracted delivery services), a GCC is required and rules concerning the requirements for residence and work permits apply. Personnel who do not live in Germany will need to provide their country's equivalent of the GCC, translated into English and notarized. This documentation must accompany the access-roster request. Under extenuating circumstances, USAG commanders may provide a local ETP to background checks required for vendors and contractors on an access roster.

(6) IACS registrars will enter access-roster information into the IACS and distribute copies of access rosters to ACPs as needed.

38. EMERGENCY-VEHICLE ACCESS

a. Access During an Emergency.

(1) During a coordinated emergency, 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 officer will notify the appropriate ACP to allow for unimpeded access.

(2) In situations where the HN emergency response has not been coordinated through the DES, 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 the purpose of the entry and notify the MP desk officer.

(3) Ambulance service is provided by HN hospitals. USAGs should include a description of HN ambulances in their local 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. USAGs 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 servicing U.S. Forces police for guidance (for example, MP desk officer).

(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 *Official Guest* category (para 22) to access the installation.

c. Other HN Service Providers. USAGs 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. USAGs should develop memorandums of agreement that require these service providers to notify the installation ahead of time when access is required.

39. SPECIAL-VEHICLE ACCESS

a. Protective-Services Vehicles.

(1) Protective-services heavy armored vehicles (HAVs) (commonly called “hard cars”) and security-escort vehicles (SEVs) (commonly called “chase cars”) do not have blanket authority to enter closed installations without presenting proper credentials.

(2) ACP guards will not stop HAVs or SEVs that have been granted unimpeded access through coordination with the responsible DES. 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 with the DES 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 ID. Exceptions to this requirement are made on an installation basis and must be approved by the USAG 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) The primary treaties to which U.S. organizations in Europe are subject include the Treaty on Conventional Armed Forces in Europe; the Vienna Document 1999; and the Treaty on Open Skies. According to AE Regulation 525-50, the treaty-compliance officer will notify USAGs of inspections and coordinate access for teams conducting treaty-compliance inspections under these and other treaties. Inspection teams will arrive at U.S. installations under escort in vehicles provided by the HN.

NOTE: 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 by the applicable treaty. During treaty inspections, inspectors operate under diplomatic immunity and, consequently, may not be searched again by gate guards or military law-enforcement or security personnel.

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

c. USAG Shuttlebuses Transiting Between IACS-Controlled Installations (During FPCON Bravo Only).

(1) USAG commanders may use the Trusted Traveler Program (glossary) as outlined in the USEUCOM Antiterrorism (AT) OPORD 16-03, appendix 1 to annex N, Installation Access, paragraph 3c(5)(d)7. The program provides for the following:

(a) If the bus driver has a DOD ID card, the ACP guard will scan the ID card and the driver will vouch for the security of the bus.

(b) If the bus driver has a U.S. Forces in Europe installation pass, the ACP guard will scan the driver's installation pass and one passenger DOD ID card. The passenger will vouch for the fact that the bus did not stop between installations.

(2) USAGs will suspend this policy during random AT measures.

(3) ACP guards may decide to scan all passengers on the bus if an unusual situation exists.

40. ACP GUARDS

a. ACP guards will—

(1) Perform their duties in accordance with this regulation, AE Regulation 190-13, USEUCOM Physical Access Control System Identity Proofing SOPs, and the USEUCOM Encounter-Management SOP.

(2) Grant access only to individuals authorized access according to the policy and procedures in this regulation. 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 39. Table 1 lists the appropriate actions based on responses from handheld scanners.

NOTE: The IACS LEO module at the MP desk is used to determine actions for flagged IACS records.

(3) Follow the escorted-visitor paper-pass policy and procedures in paragraph 36 and do the following:

(a) Ask individuals who are not U.S. citizens or permanent residents of the United States to read AE Form 190-16E (in English, German, or Italian, whichever language is required) and sign the form or visitor log book (manually or, if available, electronically). As a minimum, the visitor book will provide space for last and first 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 for the required length of the visitor paper pass (1 to 3 days or as authorized by local policy).

(f) Complete the visitor-pass application process.

(g) Print and have the visitor sign the escorted-visitor paper pass.

(h) 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.

(4) Follow the access-roster policy and procedures in paragraph 37.

NOTE: All personnel conducting access control may confiscate DOD ID cards or installation passes using AE Form 190-16B (para 5f(8) and table 1). USAGs will establish receipt procedures for individuals whose cards or passes are confiscated as well as procedures to ensure these documents are turned in to the servicing IACO or ID-card issuing facility as appropriate. The receipt for a confiscated or expired DOD ID card or installation pass cannot be used as an authorized access document.

b. If 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).

c. When the IACS is operational at an ACP, guards will scan 100 percent of DOD ID cards and installation passes unless emergency vehicles (para 38) or special vehicles (para 39) require access or Trusted Traveler procedures are active.

NOTE: Trusted Traveler procedures are not in effect during FPCONs Charlie and Delta.

d. If scanning reveals that an installation-pass holder or DOD ID cardholder is not registered in the IACS and the installation pass or DOD ID card was issued that same day, access may be granted to the installation.

e. If a DOD ID card or CAC issued to a U.S. citizen is not registered in the IACS, the guard will—

(1) Ask for a second form of photo ID (for example, drivers license).

(2) Take the DOD ID card or CAC, the second form of photo ID, and any supporting document (for example, TDY orders, approved leave request) and log the entry into the IACS.

(3) Return the documents and inform the individual to register in the IACS.

NOTE: If an individual does not have a second form of photo ID and is over the age of 18, the guard will deny access.

f. If a DOD ID cardholder or installation-pass holder has forgotten his or her card or pass, guards will ask for a second form of ID and, if available, use the IACS manual-lookup feature at the ACP to positively identify the individual and allow and record the access.

g. During gate operations, minors under the age of 10 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 will vouch for the infant's or child's identification (for example, a DOD ID cardholder with a mini-van carrying children).

NOTE: If the situation is not normal or routine, the guard is 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.

Table 1
Guard Actions Based on Scanned Responses From Handheld Scanners

Main Message	Supporting Message	Description	Action
STOP	BARRED	This person's record has been flagged as "barred" in the Defense Biometric Identification System (DBIDS) IACS database.	Do not allow onto the installation. Detain the individual and the vehicle and call law-enforcement officials. **DOD ID Card:** If the card has expired, confiscate the card and issue AE Form 190-16B to the individual. **Installation Pass:** Confiscate the pass and issue AE Form 190-16B to the individual. If the individual protests access denial, issue AE Form 190-16G.
STOP	CALL LAW ENFORCEMENT	This person's record has been flagged as "call law enforcement" in the DBIDS-IACS database.	Detain the individual, vehicle, and all occupants of the vehicle and call law-enforcement officials for instructions listed in the "Remarks" section of the IACS LEO module lookup "Search IACS Registered Persons Records."
STOP	RECORD ARCHIVED	The DBIDS-IACS record associated with this card was archived. **NOTE:** If the DOD ID card or installation pass was recently entered into IACS (within the last 24 hours) and the IACS is operational at the ACP, allow on the installation.	**DOD ID Card:** If there are no instructions and the card appears to be valid, and the individual has another form of photo ID, allow onto the installation and instruct the individual to proceed to the IACO to correct the problems with his or her ID card. If the DOD ID card is expired, confiscate the card and issue AE Form 190-16B to the individual. If there are extenuating circumstances, contact the MP desk for additional instructions. **Installation Pass:** If there are no instructions, do not allow onto the installation. Confiscate the pass and issue AE Form 190-16B to the individual.
STOP	ID CARD REPORTED LOST OR STOLEN	This person's ID card has been flagged as "lost or stolen" in the DBIDS-IACS database.	Do not allow onto the installation. Detain the individual and the vehicle, call law-enforcement officials, confiscate the ID card or installation pass, and issue AE Form 190-16B to the individual.
STOP	MULTIPLE RECORDS RETURNED	There are multiple records in the DBIDS-IACS database associated with this card.	If the ID card appears to be valid and the individual presents another form of ID, allow onto the installation and instruct the individual to proceed to the IACO to correct the problems with his or her ID card.
STOP	ACCESS DENIED AT THIS FPCON	The person has an active DBIDS-IACS record, but is not allowed access at the current FPCON.	Do not allow onto the installation.
STOP	ACCESS DENIED TO THIS INSTALLATION	This person has an active DBIDS-IACS record, but is not allowed access to this installation.	Only allow onto the installation if the individual provides additional documentation justifying access (for example, TDY or other official orders specifying this installation) or if the individual is a *Family member* (paras 25 and 26) or an installation-pass holder accompanied by a DOD ID cardholder.

Table 1
Guard Actions Based on Scanned Responses From Handheld Scanners—Continued

Main Message	Supporting Message	Description	Action
STOP	ACCESS NOT AUTHORIZED ON <day-of-week>	This person has an active DBIDS-IACS record, but is not allowed access on this day of the week.	Only allow onto the installation if the individual provides additional documentation justifying access (for example, TDY or other official orders specifying this installation) or if the individual is a *Family member* (paras 25 and 26) or an installation-pass holder accompanied by a DOD ID cardholder.
STOP	ACCESS ONLY DURING: <start-time> - <end-time>	This person has an active DBIDS-IACS record, but is not allowed access at this time of the day.	Only allow onto the installation if the individual provides documentation justifying access (for example, TDY or other official orders specifying this installation) or if the individual is a *Family member* (paras 25 and 26) or an installation-pass holder accompanied by a DOD ID cardholder.
STOP	ID CARD EXPIRED	ID card is no longer valid.	**DOD ID Card:** Verify that the DOD ID card is expired. If confirmed expired, confiscate the card and issue AE Form 190-16B to the individual. If there are extenuating circumstances, contact the MP desk for additional instructions. **Installation Pass:** Confiscate the pass and issue AE Form 190-16B to the individual.
STOP	REGISTRATION EXPIRED	The DBIDS-IACS record associated with this card has expired.	If the individual has another form of ID, allow onto the installation and instruct the individual to proceed to the IACO to update his or her ID card.
STOP	INVALID ID CARD	The security code on the ID card does not correspond to the record in the DBIDS-IACS database.	Follow the guidance in paragraphs 40e and f. Try to verify the person's registration in the IACS laptop using the manual-lookup feature. If registered, allow onto the installation. **DOD ID Card:** If not registered, ask for a second form of photo ID and supporting documentation, such as TDY orders or a leave request. Log access into IACS. Allow onto the installation and instruct the individual to proceed to the IACO to correct the problems with the ID card. **Installation Pass:** If not registered, do not allow onto the installation, confiscate the pass, and issue AE Form 190-16B to the individual. If an ID card or installation pass appears to have been tampered with, confiscate the card or pass, issue AE Form 190-16B to the individual, detain the individual, and call law-enforcement officials.

Table 1
Guard Actions Based on Scanned Responses From Handheld Scanners—Continued

Main Message	Supporting Message	Description	Action
STOP	UNABLE TO DECODE ID CARD	The IACS handheld scanner could not recognize the Code 39 barcode as one that is maintained by the DBIDS-IACS.	Follow the guidance in paragraphs 40e and f. Verify the person's registration using the IACS laptop. If registered, allow onto the installation. **DOD ID Card:** If not registered, ask for a second form of photo ID and supporting documentation such as TDY orders or a leave request. Log access into IACS. Allow onto the installation and instruct the individual to proceed to the IACO to correct the problems with the ID card. **Installation Pass:** If not registered, do not allow onto the installation, confiscate the pass, and issue AE Form 190-16B to the individual. If an ID card or installation pass appears to have been tampered with, confiscate the card or pass, issue AE Form 190-16B to the individual, detain the individual, and call law-enforcement officials.
STOP	NOT REGISTERED	The DBIDS-IACS database does not have a record associated with this card. **NOTE:** If the DOD ID card or installation pass was recently entered into IACS (within the last 24 hours) and the IACS is operational at the ACP, allow on the installation.	**DOD ID Card:** Ask for a second form of photo ID and supporting documentation, such as TDY orders or a leave request. Log access into IACS. Allow onto the installation and instruct the individual to proceed to the IACO to register his or her ID card in the IACS. **Installation Pass:** Do not allow onto the installation, confiscate the pass, and issue AE Form 190-16B to the individual.

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

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

Supplementary Agreement to the North Atlantic Treaty Organization Status of Forces Agreement

Treaty on Conventional Armed Forces in Europe

Treaty on Open Skies

Vienna Document 2011

Homeland Security Presidential Directive (HSPD) 6, Integration and Use of Screening Information to Protect Against Terrorism

HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors

Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons

Immigration and Nationality Act (Public Law (P.L.) 82-414)

Privacy Act of 1974 (P.L. 93-579)

Enhanced Border Security and Visa Reform Act of 2002 (P.L. 107-173)

5 USC 552, Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

10 USC 3013, Secretary of the Army

10 USC 5013, Secretary of the Navy

10 USC 8013, Secretary of the Air Force

DOD Instruction 8500.01, Cybersecurity

Directive-Type Memorandum 09-012, Interim Policy Guidance for DOD Physical Access Control

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

AR 25-2, Information Assurance

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 190-13, The Army Physical Security Program

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

AR 340-21, The Army Privacy Program

AR 381-45, Investigative Records Repository

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

USEUCOM Antiterrorism Operations Order 16-03

AE Regulation 25-400-2, Army in Europe Records Information Management

AE Regulation 27-9, Misconduct by Civilians

AE Regulation 27-10, Military Justice and Legal Operations

AE Regulation 190-1, Driver and Vehicle Requirements and the Installation Traffic Code for the U.S. Forces in Germany

AE Regulation 190-13, USAREUR Physical Security Program

AE Regulation 525-13, Antiterrorism

AE Regulation 525-50, Arms Control Compliance

AE Regulation 600-700, Identification Cards and Individual Logistic Support

AE Regulation 604-1, Local National Screening Program in Germany

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

AE Regulation 690-64-G, *Verhaltensregeln, Korrekturmaßnahmen, Kündigungsverfahren und Beschwerden (Ortsansässige Arbeitnehmer in der Bundesrepublik Deutschland)*

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

SECTION II
FORMS

SF 50, Notification of Personnel Action

SF 135, Records Transmittal and Receipt

DD Form 2 (RES RET), United States Uniformed Services Identification Card (Reserve Retired)

DD Form 448, Military Interdepartmental Purchase Request

DD Form 577, Appointment/Termination Record – Authorized Signature

DD Form 1173, Uniformed Services Identification and Privilege Card

DD Form 1173-1, Department of Defense Guard and Reserve Family Member Identification Card

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

DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card

DD Form 2875, System Authorization Access Request (SAAR)

DA Form 31, Request and Authority for Leave

DA Form 3434, Notification of Personnel Action - Nonappropriated Funds Employee

DA Form 3953, Purchase Request and Commitment

DA Form 5305, Family Care Plan

AE Form 190-16A, Application for Installation Access

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

AE Form 190-16C, Record of Destruction

AE Form 190-16E, Data Protection Statement and Consent to the Collection, Storage, and Use of Personal Data

AE Form 190-16F, Installation Access Control System (IACS) Access-Roster Request and Multiple (4 or More) Contractor Common Access Card (CAC) IACS Registration

AE Form 190-16G, Installation Access Redress Application

AE Form 190-16H, Installation Access Control System (IACS) Notification Letter —Access Denial

AE Form 190-16I, Installation Access Control System (IACS) Notification Letter—Assignment of Redress Control Number

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

AE Form 190-45D, Military Police Record Check

AE Form 550-175K, U.S. Forces Status Verification/*Statusnachweis für Versorgungsberechtigte Personen der US-Streitkräfte*

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

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

AE Form 604-1B, Security Questionnaire for a Simple Security Check

Air Force Form 357, Family Care Certification

APPENDIX B
HEIGHT AND WEIGHT CONVERSION CHARTS

Weight-Conversion Chart (2.2045 pounds = 1 kg)			Height-Conversion Chart (.39370 inches = 1 cm)		
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
INSTALLATION ACCESS CONTROL SYSTEM DATA PROTECTION

C-1. GENERAL
Installation Access Control System (IACS) data contains personally identifiable information (PII) and is protected by the Privacy Act of 1974 and European Union (EU) and host-nation (HN) data-protection laws (app D). The IACS is a physical-security system that provides commanders an additional layer of security by electronically vetting installation access. The use and release of IACS data is governed by AR 340-21 as well as EU and HN data-protection principles. Since IACS data is protected, it cannot be used for administrative purposes such as tracking individuals, issuing drug-testing notifications, or enforcing payment of traffic, phone, utilities, or other debts.

C-2. RELEASE OF IACS DATA
IACS data may be approved for release under very limited conditions. Examples are as follows:

a. Data is required by law based on an appropriate legal review.

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

c. 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).

NOTE: 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 law-enforcement personnel will not release data directly to HN representatives.

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

a. Be submitted in writing.

b. Be sent by encrypted e-mail to the responsible United States Army garrison directorate of emergency services; the Defense Manpower Data Center–Europe; or the Office of the Provost Marshal (OPM), HQ USAREUR.

c. 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 believes the information should be provided. Such cases require a legal review by the Office of the Judge Advocate, HQ USAREUR, before data is released.

d. 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 IG to conduct an audit to determine compliance with Directive-Type Memorandum 09-012 (app A)).

C-4. UNIQUE RFIs

a. Authorized law-enforcement 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: An RFI submitted—

a. To determine if an individual broke base restrictions.

b. By a supervisor who wants to know when an employee entered the base (time-clock stamp).

c. By an individual who wants to track Family or spouse movements.

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

a. Relating to a felony or serious crime committed on an installation.

b. Supporting an attempt to locate a missing or runaway child.

c. Relating to a Soldier who has been documented as being absent without leave.

d. Submitted by the Trial Counsel, the Criminal Investigation Division, or military police in support of a court-martial.

APPENDIX D
PRIVACY ACT AND DATA-PROTECTION STATEMENTS

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

Authority: 5 USC 301, Departmental Regulations; 10 USC 113, Secretary of Defense, Note at Public Law (P.L.) 106-65; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 18 USC 1029, Fraud and Related Activity in Connection With Access Devices; 18 USC 1030, Fraud and Related Activity in Connection With Computers; 40 USC, Information Technology Management; 50 USC, Chapter 23, Internal Security; P.L. 99-474, Computer Fraud and Abuse Act of 1986; P.L. 100-235, Computer Security Act of 1987; P.L. 103-398, Government Information Security Act; Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons.

Principal purpose(s): To identify persons authorized routine or recurring access to U.S.- or host-nation-controlled military installations.

Routine use(s): Those permitted under 5 USC 552a(b) (Privacy Act) and as specifically allowed outside the DOD pursuant to 5 USC 552a(b), and for physical-security and identity-verification purposes as stated in the system of records notice about the Defense Biometric Identification System (DBIDS) 10 published in the Federal Register.

Disclosure: Voluntary; however, failure to provide any item of information may result in continued denial of entry onto U.S.- or host-nation-controlled military installations.

Data-Protection and -Use Statement (For Non-U.S. Persons)

The personally identifiable information (PII) you provide will be protected. Your PII will be used for identification to make an access decision. It will be checked against information in U.S. and host-nation law-enforcement and antiterrorism databases. A match with information in those databases will result in access denial.

The PII you provide will be stored locally and protected against unauthorized access. PII will be used only for the purpose for which it was collected unless other purposes were authorized by law. It will be stored for 3 years in electronic and paper format.

Providing PII is voluntary; however, failure to provide any item of the required information may result in continued denial of entry onto U.S.- or host-nation-controlled military installations.

APPENDIX E
ADJUDICATION STANDARDS AND PROCEDURES USING BACKGROUND CHECKS FOR TEMPORARY AND PERMANENT INSTALLATION PASSES

E-1. PURPOSE
This appendix establishes the minimum adjudication standards to be used by United States Army garrison (USAG) commanders and Italian base commanders when determining an individual's fitness to access an installation. The purpose is to standardize the review of adverse information within the USAREUR area of responsibility. USAG and Italian base commanders may add to these standards.

E-2. REFERENCES (APP A)

a. Army Directive 2014-05, enclosure 2.

b. USEUCOM Antiterrorism Operations Order 16-03, appendix 1 to annex N.

c. AE Regulation 27-9.

d. AE Regulation 27-10.

E-3. POLICY
For individuals requesting a temporary or regular U.S. Forces in Europe Installation Pass that requires a background check, USAG 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 have 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. Barment. The individual is barred by a USAG 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., host-nation (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 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 USAG 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 AE Regulation 27-9 or AE Regulation 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 USAG civilian misconduct office to the USAG 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. The following information should be included in or 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.

b. USAG commanders or Italian base commanders will review individual packets and determine whether or not to overturn their access-denial decision.

c. If a USAG commander's or Italian base commander's review results in no change to the denial, he or she will issue a letter 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 USAG commander or Italian base commander grants a waiver to the barment, the USAG civilian misconduct office will send a copy of the waiver to the DMDC-Europe helpdesk at *usarmy.badenwur.usareur.list.opm-iacs-help-desk@mail.mil* to update the individual's IACS record.

APPENDIX F
USEUCOM ENCOUNTER MANAGEMENT

F-1. PURPOSE
This appendix establishes the USEUCOM redress procedures for individuals who were denied installation access because the Installation Access Control System (IACS) identified them as a match or potential match on the USEUCOM IACS Watchlist. The Office of the Provost Marshal (OPM), HQ USAREUR, is the proponent for the USEUCOM IACS Watchlist and provides oversight for USEUCOM encounter-management operations.

F-2. REFERENCES

a. Homeland Security Presidential Directive (HSPD) 6, Integration and Use of Screening Information to Protect Against Terrorism.

b. USEUCOM Antiterrorism Operations Order 16-03.

F-3. POLICY
Individuals identified as unfit for installation access (for example, individuals being absent without leave, deserters, individuals who have used a stolen passport or national ID, individuals for whom INTERPOL has issued a Red Notice) are denied access by their placement on the USEUCOM IACS Watchlist. Individuals who want to redress their access denial may request AE Form 190-16G from the gate guard or registrar. The OPM will coordinate the review of the information provided on AE Form 190-16G and will reply using either the AE Form 190-16H or AE Form 190-16I.

a. AE Form 190-16H. AE Form 190-16H will be issued to the requester after a review of all available records has been conducted and a determination has been made that no changes or corrections to the access denial are warranted. The individual is told not to attempt to enter any U.S. or host-nation military installations again.

b. AE Form 190-16I. AE Form 190-16I will be issued to the requester after a review of all available records has been conducted and a determination has been made that similar data matches were occurring between the requester's personal data and that of an individual who was identified as not authorized on any installation. The requester is assigned a redress control number (RCN). He or she is also told to keep the AE Form 190-16I and provide it to the gate guard if the guard asks for the RCN.

GLOSSARY

SECTION I
ABBREVIATIONS

AAFES-Eur	Army and Air Force Exchange Service, Europe
ACP	access-control point
AEPUBS	Army in Europe Library & Publishing System
AOR	area of responsibility
AT	antiterrorism
CAC	common access card
COR	contracting officer's representative
DBIDS	Defense Biometric Identification System
DCG, USAREUR	Deputy Commanding General, United States Army Europe
DD	Department of Defense
DEERS	Defense Enrollment Eligibility Reporting System
DES	directorate of emergency services
DFMD	digitized fingerprint minutia data
DOCPER	Department of Defense Contractor Personnel Office, Civilian Personnel Directorate, Office of the Deputy Chief of Staff, G1, Headquarters, United States Army Europe
DOD	Department of Defense
EEA	European Economic Area
EU	European Union
FMWR	Family and morale, welfare, and recreation
FPCON	force-protection condition
GCC	Good Conduct Certificate
HAV	heavy armored vehicle
HQ USAREUR	Headquarters, United States Army Europe
HSPD	Homeland Security Presidential directive
IACO	installation access control office
IACP	Installation Access Control Program
IACS	Installation Access Control System
ID	identification
IMCOM-Europe	United States Army Installation Management Command Europe
KO	contracting officer
LEO	law-enforcement official
LN	local national
LNSP	Local National Screening Program
MIPR	military interdepartmental purchase request
MP	military police
MRZ	machine-readable zone
NATO	North Atlantic Treaty Organization
OPM	Office of the Provost Marshal, Headquarters, United States Army Europe
P.L.	Public Law
POC	point of contact
POV	privately owned vehicle
PR&C	purchase request and commitment
RA	requiring activity
RAPIDS	Real-Time Automated Personnel Identification System

RSO	regional security officer
SCOR	site contracting officer's representative
SEV	security-escort vehicle
SF	standard form
SFMIS	Security Forces Management Information System
SOFA	[North Atlantic Treaty Organization] Status of Forces Agreement
SOP	standing operating procedure
SSM	site security manager
SSN	Social Security number
TDY	temporary duty
TPU	troop program unit
TV AL II	*Tarifvertrag vom 16. Dezember 1966 für die Arbeitnehmer bei den Stationierungsstreitkräften im Gebiet der Bundesrepublik Deutschland*
U.S.	United States
USAFE/AFAFRICA	United States Air Forces in Europe/United States Air Forces Africa
USAFRICOM	United States Africa Command
USAG	United States Army garrison
USAREUR	United States Army Europe
USAREUR G2	Deputy Chief of Staff, G2, United States Army Europe
USAREUR PM	Provost Marshal, United States Army Europe
USC	United States Code
USEUCOM	United States European Command

SECTION II
TERMS

access roster
A temporary list of approved individuals authorized unescorted access to an installation

applicant
An individual applying for installation access

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

Aufenthaltstitel
Document issued in Germany to individuals who are not citizens of a European Union 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 17 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.

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

controlled-access installation
A U.S. Forces installation where access is controlled by guards

encounter-management program
A program designed to deny access to individuals identified as unfit for installation access. Individuals are identified as unfit when the Installation Access Control System (IACS) detects a direct or possible match against the USEUCOM IACS Watchlist or when the IACS is flagged with a "call law-enforcement" message.

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

first or emergency responder
An individual who is authorized access to an installation during force protection condition Delta because of the services he or she 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 assumes parental rights, duties, and obligations without going through the formalities of legal adoption

installation access control office
An office at a United States Army garrison authorized to register individuals in the Installation Access Control System and 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

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

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
A DOD ID cardholder who is authorized to request an installation pass for an individual, but is not authorized to perform sponsoring-organization responsibilities. The requester status applies only to the *Personal-Service Employee* category (basic reg, para 23) and the two *Visitor* categories (basic reg, paras 25 and 26) of the Installation Access Control System.

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

Trusted Traveler Program
A program United States Army garrison commanders may implement in accordance with USEUCOM Antiterrorism Operation Order 16-03, appendix 1 to annex N, under which DOD ID cardholders registered in the Installation Access Control System are authorized to vouch for passengers in their vehicles who have a valid form of photo ID

unserviceable
Any condition or change to a DOD ID card or installation pass that impairs a guard's ability to verify that the card- or passholder 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 card- or passholder 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