Headquarters
United States Army Europe
United States Army Installation Management Command
Europe Region
Heidelberg, Germany

Army in Europe
Regulation 190-16*

11 January 2010

Military Police

Installation Access Control

***This regulation supersedes AE Regulation 190-16, 22 March 2005, and rescinds AE Form 190-16D.**

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:

MARK A. BELLINI
Brigadier General, GS
Acting Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes policy and procedures for installation access control to U.S. Forces installations in the European theater. This regulation does not apply to restricted areas governed by other regulations (AR 190-13).

Summary of Change. This revision—

● Incorporates administrative changes throughout.

● Changes the reference for the physical design of access-control points from Technical Manual 5-853-2 to AE Regulation 190-13 (para 4a).

● Clarifies access procedures for valid visitor installation-pass holders when the visitor must temporarily exceed his or her access level and is accompanied by a DOD ID cardholder (para 8a(2)(c)).

● Provides sign-in privileges to military spouses under the age of 18 (para 9d).

● Updates information on next-generation common access cards (CACs) (para 10b).

● Renames the category Contractor (Living in Host Nation) to Contractor (Resident of European Union (EU) or NATO-Member Country) (para 12).

● Adds organizations to perform sponsoring-organization responsibilities when access to more than three direct-report garrisons is requested (para 12d(2)(a)).

● Updates the Contractor (U.S. Citizen Working for a U.S. Company Based in the United States) category to comply with German tax-law requirements (para 13).

● Applies local national sign-in restrictions at force protection condition (FPCON) Charlie (para 18j).

● Limits passes for local national personnel who have sign-in privileges to 24 months (para 20c).

● Clarifies the definition of the NATO member category and the age limit of dependent Family members (para 22a).

● Adds that new civilian hires who cannot immediately receive a CAC will receive a temporary installation pass in the category of official guest (para 23a(8)).

● Updates the definitions of Official Guest (para 23), Visitor (Immediate Family Member Living in Europe) (para 26), and Visitor (Friend or Family Member Not Included in Category Above) (para 27).

● Clarifies that stamped signatures are not acceptable on AE Form 190-16A (para 29c(2)(e)).

● Updates information on the commander's adjudication responsibilities for individuals with adverse background checks and the adjudication process (para 29c(5)).

● Updates information on the new *Aufenthaltstitel* (residence certificates) issued in Germany (para 29c(6)(c)).

● Requires citizens from certain countries identified by the United States Department of State to obtain the approval of the applicable garrison commander for garrison access, and the approval of the applicable garrison commander and the USAREUR Provost Marshal for Army in Europe-wide access (para 29c(11)).

● Requires that AE Form 190-16E (when approved) to be signed and included in completed application packets for filing (para 29g).

● Allows requests for new installation passes to be processed 45 days before the current pass expires, and allows installation access control offices (IACOs) to issue a pass 90 days after the original pass expires if an individual has a valid reason for being unable to renew his or her pass (for example, because of illness, injury, temporary duty) (para 31a).

● Authorizes IACOs to further extend temporary installation passes if Local National Screening Program results are not returned after the first 90-day extension (para 33a). (This authorization was formerly restricted to the USAREUR Provost Marshal.)

● Incorporates DCG, USAREUR-approved Installation Access Review Process Action Team input on the sponsor's responsibility to ensure signed-in individuals are escorted at all times (para 37e).

● Updates access-roster policy to allow individuals with a current Police Good Conduct Certificate to be placed on the access roster multiple times as long as their installation access is nonrecurring and not regularly scheduled (for example, oncall repair personnel) (para 38).

● Adds that access-roster requests (AE Form 190-16F) may be sent electronically from a .nato e-mail address and from specific USAREUR-affiliated organizations (for example, Army and Air Force Exchange Service, Europe; Defense Commissary Agency, Europe; United States Army Medical Department activities) (para 38h(2)).

● Clarifies policy on installation access for emergency and protective services vehicles (paras 39 and 40).

● Add procedures for providing access to Arms Control Treaty vehicles (para 40b).

● Adds appropriate actions for installation guards for scanned responses from the handheld scanner (table 1).

● Adds the German version of the installation-pass holder acknowledgement of responsibilities (app D).

● Emphasizes that adequate justification must be provided on applications for installation passes.

● Adds FPCON Charlie and Delta restrictions for installation-pass categories.

● Reduces the length of time an installation pass is valid to 2 years for the following person categories:

  ○ Host-Nation Government Official.

  ○ Host-Nation Military Member.

  ○ NATO Member.

  ○ Visitor (Immediate Family Member Living in Europe).

● Updates AE Form 190-16A to incorporate FPCON changes.

Applicability. This regulation applies to personnel requiring access to U.S. Forces-controlled installations in Europe. This regulation does not apply nor is it intended to restrict or limit the authority of commanders of contingency bases or bases operating in austere environments for organizing their force protection and executing their mission in a manner consistent with established plans and operations.

Supplementation. Organizations will not supplement this regulation without USAREUR Provost Marshal (PM) (AEAPM-SO) 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, and AE Form 190-16F. AE and higher level forms are available through the Army in Europe Publishing System (AEPUBS).

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 available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this regulation is the USAREUR PM (AEAPM-SO, DSN 381-7427). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR PM (AEAPM-SO), Unit 29931, APO AE 09086-9931.

Distribution. A (AEPUBS).

CONTENTS

SECTION I
GENERAL

1. PURPOSE
This regulation—

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

b. Provides IACS registration procedures.

c. Provides procedures for preparing and issuing installation passes.

d. Must be used with the following regulations:

(1) AR 25-400-2.

(2) AE Regulation 25-400-2.

(3) AE Regulation 190-13.

(4) AE Regulation 525-13.

(5) AE Regulation 600-700.

(6) AE Regulation 604-1.

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. Information on the physical design of an access-control point (ACP) may be found in AE Regulation 190-13 or provided by the installation antiterrorism officer, the physical security officer, or 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 ID card (common access card (CAC)) or installation pass.

(2) The ability to implement force protection condition (FPCON) measures Army in Europe-, CNE-C6F, or USAFE-wide, or at garrison or installation level.

(3) The centralized control of access privileges. For example, sponsors may withdraw a terminated employee's access authorization, commanders may bar individuals, and 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 (paras 12 through 28).

5. RESPONSIBILITIES

a. The USAREUR G2 will—

(1) Manage the Local National Screening Program (LNSP) (AE Reg 604-1).

(2) Provide an automated system to support the local national (LN) screening process.

b. The USAREUR G3 will—

(1) Coordinate changes to AE Regulation 525-50 concerning installation access for inspection teams.

(2) Ensure required notifications are made for installation access before the inspection team arrives.

c. The Inspector General, USAREUR, will include sponsor responsibilities as an area of special interest when inspecting organizations that sponsor installation-pass holders.

d. The Provost Marshal (PM), USAREUR, will—

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

(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 exceptions to policy.

(4) Coordinate the access authorization decision with the sponsoring organization for all installation-pass applications when the results of any background check indicate derogatory information and Army-in-Europe-wide access is requested.

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

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

(7) Provide oversight for the procurement and security of installation-pass cardstock.

(8) Perform automated audits on IACS-user activity.

(9) Coordinate with IMCOM-Europe and United States Army garrisons (USAGs) to ensure that the IACS database accurately shows all barred individuals.

e. The Director, IMCOM-Europe, will—

(1) Ensure that recipients of AE Form 600-700A understand that the form is not an installation-access document and that they must obtain an installation pass according to this regulation to enter U.S. Forces-controlled installations.

(2) Provide the central depository for Army-in-Europe-wide bars to installations and develop procedures for providing timely updates to bar rosters so that the IACS remains current and accurate.

f. Direct-report garrison (DRG) commanders will—

(1) Develop policy to ensure access to indirect-report garrisons (IRGs) is controlled according to this regulation. USAG installation-access control policy must not circumvent this regulation. For example, DRG commanders will not develop policy that honors only installation passes issued by their DRG or one of their subordinate IRGs. The intent of the Installation Access Control Program is for authorized access documents to be accepted at all U.S. Forces installations, regardless of where the access document was issued.

(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 when the results of the background check include derogatory information. This may be delegated to the IRG when access is limited to a single IRG.

(4) Develop an adjudication policy and process when an applicant has derogatory information from his or her background check (para 29c(5)(c). If an applicant requests access to more than one DRG and the commander recommends approval, the DRG will send the results to the USAREUR PM (AEAPM-SO), Unit 29931, APO AE 09086-9931 (fax DSN 381-8140) for adjudication.

(5) Develop procedures to notify the USAREUR PM of bars originating from a DRG that are not Army-in-Europe-wide bars.

(6) Execute sponsoring-organization responsibilities where this regulation designates the DRG as the sponsoring organization.

(7) Consult the USAREUR PM on access options when access methods authorized by paragraph 8a do not adequately support co-use agreements with the host nation.

g. In addition to the responsibilities in subparagraph e above, USAG commanders in Belgium, Italy, and the Netherlands will adapt the policy and procedures of this regulation to meet their unique host-nation laws as needed (for example, requirements for background checks, obtaining fingerprints, vehicle registration, *Aufenthaltstitel*). 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 USAREUR PM and the Judge Advocate (JA), USAREUR.

h. IRG commanders will—

(1) Establish policy and procedures to enforce the provisions of this regulation in their areas of responsibility (AORs). This includes but is not limited to the following requirements:

(a) Procedures for DOD ID cardholders to register in the IACS during inprocessing at either their servicing IACO or the central processing facility (CPF).

(b) Procedures for retrieving installation passes or DOD ID cards from individuals who no longer require installation access or who have unserviceable or expired installation passes or DOD ID cards. AE Form 190-16B is provided to installation-pass or ID cardholders when their installation pass or ID card is confiscated. Confiscated DOD ID cards may not be destroyed. They must be provided to the nearest DOD ID-card issuance facility for proper disposition within 24 hours after they are confiscated.

(c) A policy for IACOs to develop standing operating procedures (SOPs) that support this regulation.

(d) A policy for ACPs to have special guard orders that meet the scope and intent of this regulation. As a minimum, these special guard orders must include the following:

1. Instructions for sign-in procedures, access rosters, emergency and protective services vehicles, and processing nonregistered DOD ID cardholders.

2. Instructions for handling unique access requests not covered by this regulation.

3. Instructions for conducting manual checks of access documents if IACS operations are disrupted.

(2) Provide a copy of the ACP policy ((d) above) to the responsible works councils.

(3) Ensure only authorized users have access to the IACS. Authorized users will be designated in writing with their user level (for example, registrar or super-registrar).

(4) Provide an IACS-generated report with the names of individuals who are barred from entry to U.S. Forces installations to hiring agencies in their AOR. This report must be provided at least quarterly and when requested.

(5) Ensure proper security procedures are in place to safeguard IACS equipment at IACOs, CPFs, and ACPs.

(6) Ensure all IACS hardware transferred to the USAG is dedicated to support the IACS.

(7) Execute sponsoring-organization responsibilities where this regulation designates the IRG as the sponsoring organization.

i. USAG directors of emergency services (DESs) will—

(1) On notification of a lost or stolen DOD ID card or installation pass, immediately flag the record in the IACS to deregister the lost 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 derogatory information, copies must be sent to the sponsoring organization and the DRG. DRG policy for processing background checks that result in derogatory information must be followed.

j. 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 the contract includes requirements for background checks and an *Aufenthaltstitel* for installation passes and access rosters according to this regulation.

(2) Include a contract provision 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, the employee resigns or is terminated).

(3) Develop procedures to ensure sponsoring organizations (l below) include the following information on all purchase requests and commitments (PR&Cs), military interdepartmental purchase requests (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 requiring activity and the name and telephone number of the requiring activity's installation-access POC.

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

k. Section V explains IACO responsibilities.

l. Sponsoring organizations will ensure—

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

(2) An installation-pass application (AE Form 190-16A) is prepared for each installation-pass applicant. The application will identify the applicant's access requirements and justify these requirements as required by this regulation (for example, when sign-in privileges are requested). Failure to provide sufficient justification on the installation-pass application may result in privileges being denied or the application being rejected.

(3) Background checks are initiated and completed, and appropriate actions are taken depending on the results. When any derogatory information is discovered, the sponsoring organization must coordinate with the host DRG commander (or the USAREUR PM if Army-in-Europe-wide access is requested) to determine if the derogatory information warrants denial of the request. The USAREUR G2 must be notified if derogatory information results in the denial of access privileges.

(4) The applicant registers his or her privately owned vehicle (POV) according to 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 applicable IACO and the name and telephone number of the IACO POC.

(6) Contracting officers outside the purview of the 409th Support Brigade are informed of 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) A record of personnel sponsored by the organization and supporting documentation is maintained.

(9) A reconciliation with the servicing IACO is conducted every 6 months so that the IACS database accurately identifies individuals sponsored by the organization.

(10) A memorandum or DD Form 577 that designates persons authorized to perform sponsoring-official duties on behalf of the sponsoring organization (para 29c(2)(b)) is sent to the servicing IACO. The memorandum or DD Form 577 must be updated annually.

(11) The procedures in paragraph 29d are followed when the sponsoring official cannot escort the applicant to the servicing IACO.

m. Persons requiring recurring and unescorted access to U.S. Forces installations using a DOD ID card or installation pass will—

(1) Consent to the procedures for 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 CPF. If a DOD ID cardholder has a manually produced card, that individual 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 their person 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 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 or servicing IACO so that the card can be deregistered.

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

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

(6) Register their POVs as part of the installation-pass application process if they plan to use the 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 the requirements of this regulation are enforced. Inconvenience to individuals is not a valid reason for circumventing or modifying the procedures established by this regulation.

7. EXCEPTIONS TO POLICY

a. Exceptions to policy may be approved by the USAREUR PM for up to 1 year.

b. Persons requesting an exception to any policy or procedures in this regulation must send their request through appropriate command channels to the USAREUR PM (AEAPM-SO), Unit 29931, APO AE 09086-9931; fax DSN 381-8140; or e-mail: iacs3@eur.army.mil.

c. Exceptions to policy that is embedded in the IACS software application may be administered locally and do not require USAREUR PM approval. The USAREUR PM periodically audits and reviews software exceptions to policy.

SECTION II
INSTALLATION ACCESS

8. ACCESS METHODS

a. Personnel may obtain authorized access to U.S. Forces installations by one of the following four methods:

(1) Have a valid DOD ID card and be registered in the IACS. The following machine-produced DOD ID cards are considered valid access documents:

(a) CAC (current- or next-generation).

(b) DD Form 2(RET). This blue card is issued to military retirees.

(c) DD Form 2(RES). This green card is issued to Reserve and National Guard personnel.

(d) DD Form 1173. This tan card is issued to eligible Family members of military and DOD civilian personnel.

(e) DD Form 1173-1. This red card is issued to eligible Family members of Reserve and National Guard military personnel.

(f) DD Form 1934. This card is issued to religious, medical, and auxiliary medical personnel who serve in or accompany the U.S. Armed Forces in combat regions and who may become prisoners of war.

(g) DD Form 2765. This tan card is issued to Medal of Honor recipients and honorably discharged veterans rated by the Department of Veterans Affairs as 100-percent disabled from a uniformed service-connected injury or disease (other than current or retired members of the uniformed services).

NOTE: DD Form 2(RES RET) is a red card issued to retired members of the Reserves under the age of 60. The DOD civilian retiree card is an optional ID card without an electronic chip. Individuals issued DD Form 2(RES RET) or the DOD civilian retiree card are not covered by the NATO Status of Forces Agreement (SOFA), and their cards cannot be registered in the IACS.

(2) Have 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.

(b) Although these installation passes are similar in appearance, the restrictions associated with each are different. The 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 Police Good Conduct Certificate (PGCC) (*Polizeiliches Führungszeugnis*) or equivalent background check with no adverse results.

2. A regular installation pass is valid up to 5 years, depending on the category, and requires a PGCC or equivalent and completion of the LNSP background check with no adverse results.

NOTE: Background checks that uncover entries must be forwarded to the sponsoring organization and to the host DRG for adjudication. USAG and other commanders and security personnel will strictly control 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 of the employee for action. Paragraph 29c(5)(c) provides additional guidance.

(c) A valid installation pass with temporary duty (TDY) orders will authorize access when an individual must temporarily exceed his or her access level for operational reasons. A valid visitor installation-pass holder, when accompanied by a DOD ID cardholder, is authorized access when the individual must temporarily exceed his or her access level. The following are examples of when an increased level of access may be temporarily authorized:

Example 1: If an installation-pass holder has a USAG-Stuttgart-wide installation pass but must attend training in USAG Mannheim, his or her installation pass with TDY orders stating the training location and dates may be used to obtain access. Because not all of these situations involve the issue of TDY orders, other documents that state the purpose of the travel and the location and dates are acceptable.

Example 2: If a visitor installation-pass holder has a USAG-Ansbach-wide installation pass but accompanies a DOD ID cardholder to an installation in USAG Kaiserslautern during the course of the visit, the visitor will be allowed access to the installation without being required to sign in. A statement authorizing access will be printed on the back of the installation pass.

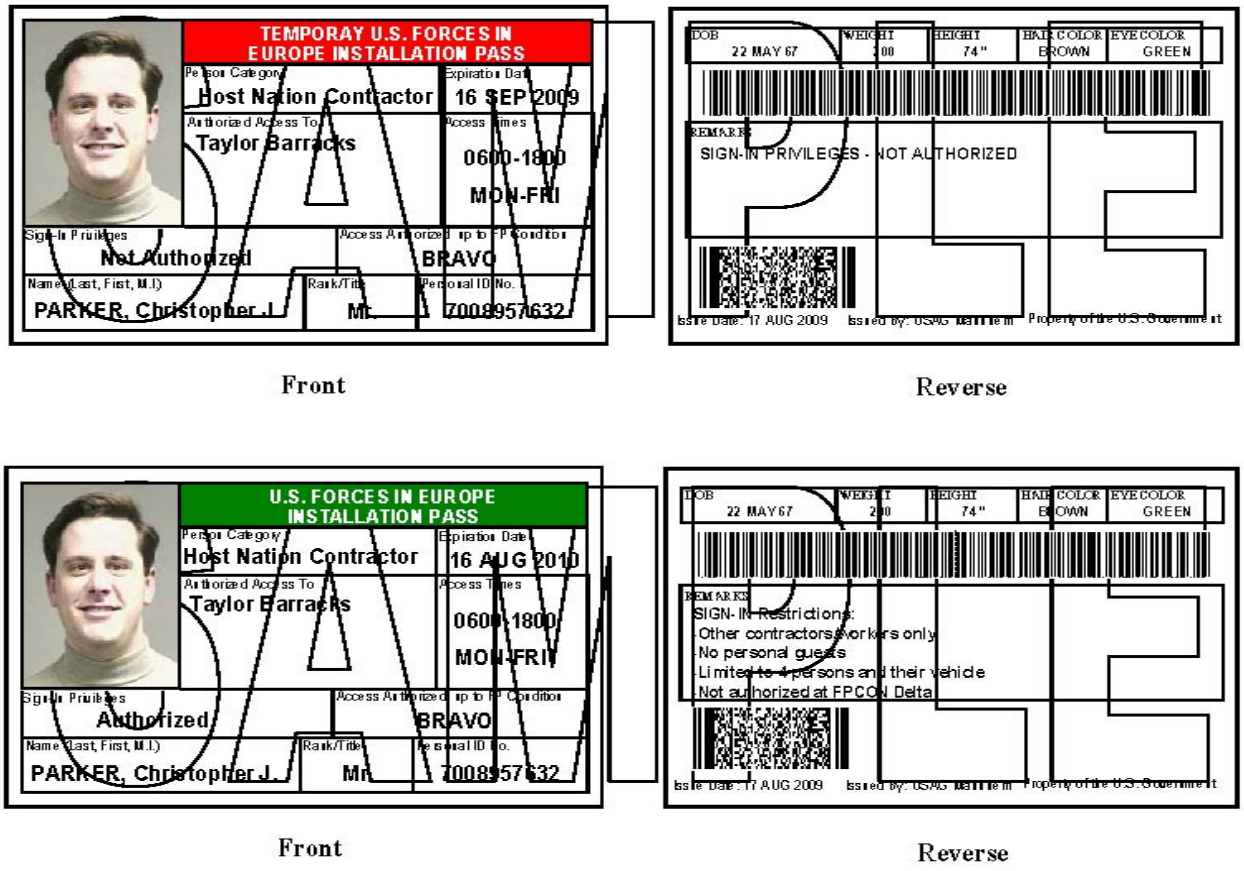

Figure 1. Sample Temporary and Regular U.S. Forces in Europe Installation Pass

(3) Be signed in by an individual with sign-in privileges and present one of the documents listed in paragraph 29e.

(4) Be on an approved access roster and present one of the documents listed in paragraph 29e and, if required, the required background check.

NOTE: There may be situations when commanders must supplement the methods 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 subparagraph a above must be defined in IRG policy and approved by the DRG commander. In these situations, the policy in paragraph 7 still applies.

b. Paragraph 39 explains access policy for emergency-vehicle access, and paragraph 40 explains policy for special-vehicle access.

c. Installation commanders will not further restrict access unless a bona fide need exists (for example, the installation has critical assets or restricted areas and there are no other layers of protection available). In these situations, commanders may determine that additional documents (such as 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).

d. Although a U.S. passport is not a valid access document, guards will not deny access to U.S. citizens who are not DOD ID card or installation-pass holders during an emergency (for example, when the FPCON changes to Delta). Under these conditions, guards will immediately contact the MP office for assistance. An MP official will meet the U.S. citizen at the ACP and provide the necessary assistance for access.

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. The following individuals may be registered in the IACS:

(1) Reserve DOD ID cardholders who are permanently assigned to the 7th Civil Support Command (7th CSC).

(2) DOD ID cardholders who are on TDY (on orders) in Europe. These individuals may be registered in the IACS for the duration of their TDY.

(3) Active duty military personnel and retirees who are visiting Europe. These individuals may be registered in the IACS for the duration of their visit, up to 90 days, or the date specified by the host-nation visa.

(4) Retired military members living in the host country. These individuals may be registered in the IACS if they have an *Aufenthaltstitel* from the host country.

(5) DOD ID cardholders (including minors) who are EU citizens but are not command-sponsored (no SOFA status). These individuals may be registered in the IACS for the duration of their stay or the expiration date of their ID card, whichever is earlier.

NOTE: Individuals who have multiple DOD ID cards (for example, a military retiree who is now a DA civilian employee or a technical expert status accreditation (TESA) contractor) must choose which DOD ID card they want to use for IACS registration and use that card to gain access to installations.

b. Documentation. DOD ID cardholders must provide documentation that supports their requirement to be registered in the IACS. This documentation will be used to determine the expiration date of the registration period. In no case will the registration period exceed 5 years.

c. Restrictions. There are no restrictions on the number of installations DOD ID cardholders may enter, on the times they may enter, or under which FPCONs they may enter unless restrictions are imposed by an authorized commander.

d. Sign-In Privileges. DOD ID cardholders are limited to signing in four persons and their vehicles, and must be at least 18 years old, except for active duty military members and their spouses. An authorized commander may reduce or deny this privilege.

e. Registering Minors. Minors must be registered in the IACS in the presence of a parent or legal guardian.

10. COMMON ACCESS CARDS

DOD has begun to issue next-generation CACs that are slightly different than the current CAC. The next-generation CAC has *Department of Defense* printed in light blue repeatedly as the background of the card. CACs issued for computer access only cannot be registered in the IACS or be used for installation access. The following guidelines will be used when registering CACs:

a. Current-Generation CAC.

(1) CACs with a vertical green stripe that say *IDENTIFICATION AND PRIVILEGES CARD* on the bottom may be registered in the IACS.

(2) CACs without a stripe may be registered in the IACS, with or without a social security number on the back.

(3) CACs with a vertical red stripe are issued to non-U.S. citizens and cannot be registered in the IACS. LN employees who have this CAC must obtain an installation pass for access according to paragraph 24.

b. Next-Generation CAC.

(1) CACs with a horizontal green stripe that have only *IDENTIFICATION CARD* on the bottom cannot be registered in the IACS.

(2) CACs with a horizontal green stripe that have *IDENTIFICATION AND PRIVILEGES CARD* on the bottom may be registered in the IACS.

(3) CACs without a stripe but with a social security number on the back may be registered in the IACS.

(4) CACs with a horizontal blue stripe cannot be registered in the IACS. The blue-striped CAC is issued to LN employees. LN employees must obtain an installation pass for access according to paragraph 20.

(5) CACs with a horizontal red stripe are issued to first-responders and may be registered in the IACS.

11. INSTALLATION PASSES

Individuals may qualify for an IACS installation pass in one of the following categories:

a. Contractor (Resident of European Union (EU) or NATO-Member Country) (para 12).

b. Contractor (U.S. Citizen Working for a U.S. Company Based in the United States) (para 13).

c. Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract) (para 14).

d. Department of State and American Embassy Personnel (para 15).

e. Foreign Student (Marshall Center) (para 16).

f. Gate Guard (para 17).

g. Host-Nation Government Official (para 18).

h. Host-Nation Military Member (para 19).

i. Local National Employee (para 20).

j. Member of Private Organization (para 21).

k. NATO Member (para 22).

l. Official Guest (para 23).

m. Personal-Service Employee (para 24).

n. Vendor (Providing Merchandise or Services Not Associated With a Government Contract) (para 25).

o. Visitor (Immediate Family Member Living in Europe) (para 26).

p. Visitor (Friend or Family Member Not Included in Category Defined in Para 26) (para 27).

q. Other (para 28).

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

a. Definition. A *Contractor* (*Resident of EU or NATO-Member Country*) is an individual without NATO SOFA status who lives in the EU or a NATO-member country, is contracted to work for DOD in Europe, and is not a DOD ID cardholder. Contractors who are trying to establish a contract with DOD may be granted access only through an individual who has sign-in privileges or through access-roster procedures.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized a temporary installation pass only after all required background checks are completed and an LNSP background check has been initiated.

(2) Regular Installation Pass. Individuals in this category may be authorized a regular installation pass after all background checks (including LNSP) have been completed and returned negative with no entries.

c. Length of Time Pass Is Valid. The temporary installation pass will be valid for the length of the contract or up to 90 days, whichever is less. The regular installation pass will be valid for the length of the contract, up to 2 years, or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements.

(1) Identifying the sponsoring organization for this category of individual may be difficult. In general, the organization hiring the contractor will perform the sponsor responsibilities in this regulation. Hiring organizations will request the minimum access level required. For example, if an organization is going to have furniture delivered to two installations in a USAG, the hiring organization will not sponsor the contractor for access beyond the two installations.

(2) Sponsoring-organization requirements for various levels of access are as follows:

(a) When access to four or more DRGs is requested, the request is considered the same as "Army-in-Europe-wide" and can be approved by the following sponsoring organizations:

1. Department of Defense Dependents Schools - Europe (DODDS-Europe).

2. Defense Commissary Agency, Europe (DECA-Europe).

3. Defense Logistics Agency - Europe (DLA-Europe).

4. Army and Air Force Exchange Service, Europe (AAFES-Eur).

5. Military Surface Deployment and Distribution Command, Europe.

6. United States Army Center for Health Promotion and Preventive Medicine - Europe.

7. United States Army Medical Materiel Center, Europe.

8. United States Army Corps of Engineers, Europe District.

9. HQ USAREUR staff offices.

10. IMCOM-Europe staff offices.

11. 21st Theater Sustainment Command.

12. United States Army Southern European Task Force.

13. Seventh United States Army Joint Multinational Training Command.

14. 7th CSC.

15. 18th Engineer Brigade.

16. 5th Signal Command.

17. 66th Military Intelligence Brigade.

18. 202d Military Police Group.

19. United States Army Europe Regional Medical Command.

20. United States Army Europe Regional Dental Command.

21. 405th Support Brigade.

22. 409th Support Brigade.

23. 1st Transportation Movement Control Agency.

24. Defense Manpower Data Center - Europe.

NOTE: The USAREUR PM will adjudicate cases when an organization other than those listed above believes that it should have Army-in-Europe-wide sponsoring authority.

(b) When access is required to three DRGs or less, the grade requirements of paragraph 29c(2)(c) apply. The sponsoring organization need not be one of the organizations in (a) above. The sponsoring organization may be the DRG where the contractor is headquartered or performs most of his or her business.

(c) Contractors whose service exceeds one IRG but is limited to one DRG may obtain an installation pass for that DRG. The sponsoring organization must be the DRG.

(d) In all other cases, sponsoring organizations are not authorized to sponsor an installation-pass applicant beyond the IRG.

(3) Contractors who are unable to obtain an installation pass based on the requirements in (2) above but who require access to installations throughout the European theater based on individual contracts with several organizations should—

(a) Obtain an installation pass for the garrison where they conduct most of their business.

(b) Use sign-in procedures or site-specific access rosters for other locations. Paragraph 38 explains access-roster requirements.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before a temporary or regular installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before a temporary or regular installation pass may be issued.

(3) LNSP. LNSP screening applies to both non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months without NATO SOFA status. This screening must be initiated before a temporary installation pass may be issued. The screening must be completed and returned negative with no entries before a regular installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* may be required for non-host nation citizens unless the individual has an exception to this requirement (para 29c(6)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations is limited to the minimum required for the contractor to perform his or her duties according to subparagraph d above.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsoring organization.

i. Restrictions on Sign-In Privileges.

(1) Sign-in privileges normally are not granted to contractors. As an exception, contractors may be granted sign-in privileges when the sponsoring official is at least a lieutenant colonel or civilian equivalent (GS-13, NSPS-3, NF 5, or C8).

(2) USAGs in Belgium, Italy, and the Netherlands may use the equivalent grade for their LN employees. Sign-in privileges are not authorized at FPCON Delta.

(3) Sign-in privileges, when authorized, are limited to signing in four people and their vehicles.

(4) Only other contractors and vendors who support the contract may be signed in.

(5) Sign-in privileges are not authorized for temporary installation-pass holders.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to the following FPCONs:

(1) Temporary installation-pass holders: Bravo.

(2) Installation-pass holders: Bravo. If identified as essential personnel: Charlie. If identified as essential personnel and first-responder: Delta.

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

a. Definition. A *U.S. Contractor* is 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. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized a temporary installation pass for up to 90 days if they provide the required documentation.

(2) Regular Installation Pass. Individuals in this category may be authorized a regular installation pass if they provide the required documentation.

c. Length of Time Pass Is Valid.

(1) The temporary installation pass will be valid for the length of the visit or up to 90 days, whichever is less. For visits to Germany, a "fax-back" 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 all required country documents are completed before obtaining a temporary pass.

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

d. Sponsor Requirements. The organization inviting or escorting the contractor will perform the sponsor responsibilities in this regulation and ensure compliance with country labor laws. In Germany, the organization must ensure compliance with policy of the DOD Contractor Personnel Office, Office of the Deputy Chief of Staff, G1, HQ USAREUR (AE Reg 715-9).

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel*. For individuals requesting an installation pass, a residence permit may be required after 90 days and a work permit may be required after 6 months (AE Reg 715-9).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations is limited to the minimum required for the contractor to perform his or her duties.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Contractors in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to the following FPCONs:

(1) Temporary installation-pass holders: Bravo.

(2) Installation-pass holders: Bravo. If identified as essential personnel: Charlie.

14. DELIVERY PERSONNEL (RECURRING DELIVERIES OR SIMILAR SERVICE NOT ASSOCIATED WITH A GOVERNMENT CONTRACT)

a. Definition. *Delivery Personnel* are 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.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized a regular installation pass after all background checks (including LNSP) have been completed and returned negative with no entries.

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

d. Sponsor Requirements. The IRG being serviced will sponsor individuals in this category.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before an installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before an installation pass may be issued.

(3) LNSP. LNSP screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. It must be completed and returned negative with no entries before an installation pass may be issued.

f. *Aufenthaltstitel*. Non-host nation citizens require an *Aufenthaltstitel*. Paragraph 29c(6)(c) explains exceptions to this requirement.

g. Restrictions on Number of Installations a Pass Holder May Enter. Installation-pass holders will not be granted access outside of the sponsoring IRG. The sponsoring IRG may impose further restrictions (for example, to only certain caserns). Access may be extended to the DRG only if the DRG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Delivery personnel are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

15. DEPARTMENT OF STATE AND AMERICAN EMBASSY PERSONNEL

a. Definition. *Department of State and American Embassy Personnel* are individuals assigned to or on duty with the Department of State, with an American Embassy in the USEUCOM AOR, or at U.S. diplomatic or consular posts according to AE Regulation 600-700.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

c. Length of Time Pass Is Valid. The installation pass will be valid for the length of the tour (not to exceed 5 years) or until the expiration date on the supporting document (for example, passport, AE Form 600-700A) that was used to obtain the installation pass, whichever is earlier.

d. Sponsor Requirements. The United States Mission, Germany, is the sponsor for individuals in this category and will perform the sponsor responsibilities. The United States Mission, Germany, will submit a memorandum designating sponsoring officials to the USAREUR PM by e-mail (iacs3@eur.army.mil). The PM will post this memorandum to the restricted portion of the IACS website for IACOs. Individuals in this category may obtain their installation pass at any IACO. Because these individuals are spread throughout Europe, their first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and IACO to obtain an installation pass according to paragraph 29.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. There are no restrictions on the number of installations a pass holder may enter.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized.

i. Restrictions on Sign-In Privileges. Individuals in this category are limited to signing in four people and their vehicles.

j. FPCON Restrictions. No restrictions apply to access to installations during heightened FPCON levels.

16. FOREIGN STUDENT (MARSHALL CENTER)

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

b. Types of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

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

d. Sponsor Requirements. Representatives from the Marshall Center will perform the sponsor responsibilities.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installation a Pass Holder May Enter. Access will be limited to installations in the USAG Garmisch AOR.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized.

i. Restrictions on Sign-In Privileges. Individuals in this category are authorized sign-in privileges.

j. FPCON Restrictions. No restrictions apply to access to installations during heightened FPCON levels.

17. GATE GUARD

a. Definition. A *Gate Guard* is a guard in a position responsible for controlling access to an installation. These are usually contracted positions where guards do not require access to the installation themselves; they conduct their work only from an ACP. This category is reserved only for individuals requiring logical access (glossary). Gate guards authorized and requiring installation access for work purposes are issued installation passes under the Contractor (Resident of European Union (EU) or NATO-Member Country) person category.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

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

d. Sponsor Requirements. The sponsoring organization is the contracting officer's representative (COR) or the DRG site contracting officer's representative (SCOR).

e. Background Checks. Background checks must be completed and verified by the Provost Marshal Division, Office of the Deputy Chief of Staff, G3, HQ USAREUR, as a condition of employment.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* may be required and will be verified by the Provost Marshal Division as a condition of employment.

g. Restrictions on Number of Installations a Pass Holder May Enter. Only logical access may be granted to gate guards.

h. Restrictions on Days and Times Access Is Authorized. Only logical access may be granted to gate guards.

i. Restrictions on Sign-In Privileges. Gate guards are not authorized sign-in privileges.

j. FPCON Restrictions. No restrictions apply to access to installations during heightened FPCON levels.

18. HOST-NATION GOVERNMENT OFFICIAL

a. Definition. A *Host-Nation Government Official* is a member of the host-nation Government who requires recurring access for official business or access based on an official relationship, or local city officials (such as the mayor, fire chief, or an employee of the German Construction Office (*Bauamt*)).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

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

d. Sponsor Requirements. The sponsoring organization will depend on the type of official guest. In most cases, the USAG will sponsor individuals in this category and will perform the sponsor responsibilities.

e. Background Checks. Background checks are not required for individuals in this category.

NOTE: Persons and firms contracted by the host nation are screened as Contractor (Resident of European Union (EU) or NATO-Member Country) and must meet the background-check requirements in paragraph 14e.

f. *Aufenthaltstitel.* An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations is limited to the minimum required for the guest to conduct official business.

h. Restrictions on Days and Times Access Is Authorized. Days and times access is authorized will be specified by the sponsoring organization.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges unless justified by the sponsoring organization. If authorized, sign-in privileges are limited to signing in four individuals and their vehicles "for official business only."

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Charlie.

19. HOST-NATION MILITARY MEMBER

a. Definition. A *Host-Nation Military Member* is a member of the host-nation military who works or resides on a U.S. Forces-controlled installation located in the country they serve (for example, German Soldiers in Germany, Italian Soldiers in Italy). This category should not be confused with the NATO Member category (para 22).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

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

d. Sponsor Requirements. If the host-nation military member works for an organization that has a DOD representative, that organization is the sponsoring organization and will perform the sponsor responsibilities. If no such organization exists, the IRG will perform the sponsor responsibilities.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel.* An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on the Number of Installations a Pass Holder May Enter. The number of installations is limited to the minimum required based on the host-nation military member's circumstances.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Installation-pass holders in this category are not authorized sign-in privileges unless sign-in privileges are justified by the sponsoring organization. If sign-in privileges are justified by the sponsoring organization, the installation-pass holder may sign in up to four individuals and their vehicles "for official business only." Sign-in privileges for installation-pass holders in this category are not authorized during FPCON Delta.

j. FPCON Restrictions. No restrictions apply to access to installations during heightened FPCON levels.

20. LOCAL NATIONAL EMPLOYEE

a. Definition. A *Local National Employee* is an individual who is employed by DOD in Europe and who is not entitled to one of the DOD ID cards listed in paragraph 8a(1). This category is primarily for host-nation employees in Europe.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized temporary installation passes after all required background checks have been completed and an LNSP background check has been initiated. The temporary installation pass will be used only until a regular installation pass is authorized.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes after all background checks (including LNSP checks (e(3) below)) have been completed and returned negative with no entries.

c. Length of Time Pass Is Valid. The temporary installation pass will be valid for up to 90 days. The regular installation pass without sign-in privileges will be valid for up to 5 years or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earlier. Installation passes with sign-in privileges will not exceed 24 months.

d. Sponsor Requirements. The organization for which the LN employee will work will perform the sponsor responsibilities in this regulation.

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before a temporary installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before a temporary or regular installation pass may be issued.

(3) LNSP. This screening applies to both non-U.S. citizens and U.S. citizens who have lived in Germany without NATO SOFA status for more than 12 consecutive months. This screening must be completed and returned negative with no entries before a temporary or regular installation pass may be issued. Employees hired before 3 October 1985 are exempt from this requirement (AE Reg 604-1). An LNSP background check is not needed if an LN employee has a current NATO or U.S. clearance.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* may be required if the applicant is not an EU resident.

g. Restrictions on the Number of Installations a Pass Holder May Enter. The number of installations an LN employee with an installation pass may enter is limited to the minimum required for the LN employee to perform his or her duties.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Temporary installation-pass holders are not authorized sign-in privileges. Installation-pass holders are not authorized sign-in privileges unless justified by the sponsoring organization. If sign-in privileges are justified by the sponsoring organization, the installation-pass holder may sign in up to four individuals and their vehicles "for official business only." Sign-in privileges for installation-pass holders are not authorized during FPCON Charlie or Delta.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to the following FPCONs:

(1) Temporary installation-pass holders: Bravo.

(2) Installation-pass holders: Bravo. If identified as essential personnel: Charlie. If identified as essential personnel and first-responder: Delta.

21. MEMBER OF PRIVATE ORGANIZATION

a. Definition. A *Member of Private Organization* is a member of an approved private organization who has no reason to enter U.S. Forces installations other than to participate in private-organization functions.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized an installation pass after all background checks (including LNSP checks (e(3) below)) are completed and returned negative with no entries.

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

d. Sponsor Requirements. The IRG where the private-organization function takes place will perform sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before an installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before an installation pass may be issued.

(3) LNSP. This screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months without NATO SOFA status. This screening must be completed and returned negative with no entries before an installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring IRG. The sponsoring IRG may impose further restrictions. Access may be extended to the DRG if the DRG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless imposed by the sponsoring IRG.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

22. NATO MEMBER

a. Definition. *NATO Members* include NATO military personnel, civilian employees, 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, and for NATO personnel assigned to an international military headquarters. This category should not be confused with the Host-Nation Military Member category (para 19).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

c. Length of Time Pass Is Valid. The installation pass will be valid for up to 2 years or for the length of the member's tour, whichever is earlier.

d. Sponsor Requirements.

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

(2) Active-Duty Belgian, British, Canadian, Dutch, and French Military ("Sending States"). The security office from the Sending State will sponsor individuals in this category. The Sending State will submit a memorandum designating sponsoring officials to the USAREUR PM by e-mail (iacs3@eur.army.mil). The PM will post this memorandum to the restricted portion of the IACS website, where it is available to all IACOs. Individuals in this category may obtain an installation pass at any IACO. Because 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 IACO to obtain an installation pass.

(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 submit a memorandum designating sponsoring officials to the USAREUR PM. The PM will post this memorandum to the restricted portion of the IACS website, where it is available to all IACOs. Individuals in this category may obtain their installation pass at any IACO. The first visit of French and British consular and diplomatic personnel to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the IACO to obtain an installation pass according to paragraph 29.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access is limited to U.S. Forces installations in the country of assignment.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized.

i. Restrictions on Sign-In Privileges. Sign-in privileges are limited to signing in four people and their vehicles.

j. FPCON Restrictions. No restrictions apply to access to installations during heightened FPCON levels.

23. OFFICIAL GUEST

a. Definition. *Official Guest* is broad category designed for individuals requiring recurring access for official business or access based on an official relationship with the U.S. Government. Examples are as follows:

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

(2) Members of clubs or organizations located on an installation (for example, shooting clubs, dance clubs, flying clubs).

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

(4) Interns participating in exchange programs or otherwise employed by USAREUR organizations. For example, Landstuhl Regional Medical Center and the United States Army Europe Regional Dental Command are regular sponsors of interns. Interns must provide visas or other documentation to receive an installation pass valid for more than 90 days.

(5) Individuals requiring access because of *in loco parentis* status or other member-of-household status. These guests are required to submit a copy of the official memorandum from the Host Nation Customs Policy Branch, Provost Marshal Division; or AE Form 600-700A.

(6) Commissary baggers who do not possess a DOD ID card. These guests will be sponsored by DECA. DECA must verify that the individuals have appropriate documentation (*Aufenthaltstitel*) before submitting them for an installation pass.

(7) Dependents of Credit Union employees. These guests are authorized access equivalent to that of a DOD ID cardholder (Army in Europe-wide access, sign-in privileges, "24/7" access) and do not require background checks. Credit Union (and other banking organizations) may not sponsor clients or customers for installation passes.

(8) New civilian hires who cannot immediately receive a CAC.

NOTE: The examples in (1) through (8) above are not all-inclusive. Sponsoring organizations will not use this category when the applicant meets the definition of another, more restrictive category.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

c. Length of Time Pass Is Valid. The temporary installation pass will be valid for up to 90 days. The regular installation pass will be valid for up to 2 years, until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, or until the expiration date of the agreement, memorandum, or membership, whichever is earliest.

d. Sponsor Requirements. The sponsoring organization will depend on the type of official guest. In most cases, the USAG will sponsor individuals in this category and perform sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before a temporary or regular installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before a temporary or regular installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations is limited to the minimum required.

h. Restrictions on Days and Times Access Is Authorized. Access times and dates are as specified by the sponsoring organization.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to the following FPCONs:

(1) Temporary installation-pass holders: Bravo.

(2) Installation-pass holders: Bravo. If identified as essential personnel: Charlie.

24. PERSONAL-SERVICE EMPLOYEE

a. Definition. A *Personal-Service Employee* is an individual hired under contract by someone (see "requester" in glossary) to perform a service (for example, as a nanny, dogsitter, housecleaner).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized temporary installation passes after all required background checks except for LNSP checks (e(3) below) have been completed.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes after all background checks (including LNSP checks (e(3) below)) have been completed and returned negative with no entries.

c. Length of Time Pass Is Valid. The temporary installation pass will be valid for the length of service or up to 90 days, whichever is earlier. The regular installation pass will be valid for the length of service, for 2 years, or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements. The IRG where the requester resides will sponsor this person and will perform sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before a temporary or regular installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before a temporary or regular installation pass may be issued.

(3) LNSP. This screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be initiated before a temporary installation pass may be issued. It must be completed and returned negative with no entries before a regular installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* may be required for non-host nation citizens unless the individual has an exception to this requirement (para 29c(6)).

g. Restrictions on Number of Installations a Pass Holder May Enter. Access may not exceed the sponsoring IRG. The sponsoring IRG may further restrict access as necessary. Access may be extended to the DRG if the DRG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the requester or sponsor.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

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

a. Definition. A *Vendor* is an individual who is authorized to offer insurance, real estate, and securities for sale, as well as merchandise (goods) and services on U.S. Forces installations (for example, ice cream or chicken truck), but is not associated with a Government contract. Vendors providing merchandise or services under Government contract (for example, AAFES, DECA, FMWR, nonappropriated fund (NAF)) are contractors and will not be placed in this category.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes after all background checks (including LNSP checks (e(3) below)) have been completed and returned negative with no entries.

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

d. Sponsor Requirements. The sponsoring organization is the IRG when the requested access does not exceed the IRG. The sponsoring organization is the DRG when access requested exceeds one IRG but is limited to one DRG. When access is for more than one DRG, the applicant must be sponsored by AAFES-Eur, DECA-Europe, or IMCOM-Europe. This sponsoring authority may not be delegated to subordinate organizations.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before an installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before an installation pass may be issued.

(3) LNSP. This screening is required for both non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be completed and returned negative with no entries before an installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* may be required for non-host nation citizens unless the citizen has an exception to this requirement (para 29c(6)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will depend on the level of the sponsoring organization (d above).

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

26. VISITOR (IMMEDIATE FAMILY MEMBER LIVING IN EUROPE)

a. Definition. A *Visitor* (*Immediate Family Member Living in Europe*) is an individual, age 10 or older, who is an immediate Family member of the requester and legally resides in the EU. In 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.

(1) Temporary Installation Pass. Individuals in this category are not authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes only when the requester resides on a controlled-access installation.

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

d. Sponsor Requirements. The USAG where the requester resides is the sponsor for individuals in this category and will perform sponsor responsibilities.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel.* An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring garrison. The sponsoring garrison may impose further restrictions. A valid visitor installation-pass holder, when accompanied by a DOD ID cardholder, is authorized access when the individual must temporarily exceed his or her access level.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

27. VISITOR (FRIEND OR FAMILY MEMBER NOT INCLUDED IN CATEGORY DEFINED IN PARA 26)

a. Definition. A *Visitor* (*Friend or Family Member*) is a visiting Family member or friend, age 10 or older, of the requester (glossary) who does not reside in the EU and is not included in the category in paragraph 26. Installation passes are not authorized in this category for local friends (including a fiance) or local residents who are not immediate Family members visiting the European theater.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized temporary installation passes.

(2) Regular Installation Pass. Family members may be authorized regular installation passes.

c. Length of Time Pass Is Valid. The temporary installation pass will be valid for the length of the visit or up to 90 days, whichever is less. The regular installation pass will be valid for the length of the visit (more than 90 days), up to 1 year, or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements. The USAG where the requester resides will sponsor individuals in this category and perform sponsor responsibilities.

e. Background Checks. Background checks are not required for individuals in this category.

f. *Aufenthaltstitel.* An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. Passes will not exceed the sponsoring IRG. The sponsoring IRG may impose further restrictions. Access may be extended to the DRG only if the DRG is willing to accept sponsoring-organization responsibilities. A valid visitor installation-pass holder, when accompanied by a DOD ID cardholder, is authorized access when the individual must temporarily exceed his or her access level.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days or times access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

28. OTHER

a. Definition. The *Other* category includes individuals who require recurring and unescorted access, but who do not meet the definition of any other person category. The USAG will review the access requirements for each applicant and evaluate the extenuating circumstances. An example of 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).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. Individuals in this category may be authorized temporary installation passes.

(2) Regular Installation Pass. Individuals in this category may be authorized regular installation passes.

c. Length of Time Pass Is Valid. The temporary installation pass will valid for up to 90 days. The regular installation pass will be valid for 1 year or until the expiration date on the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earlier.

d. Sponsor Requirements. The USAG will sponsor individuals in this category and will perform sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before a temporary or regular installation pass may be issued. USAGs in Belgium, Italy, and the Netherlands will require an equivalent police check for their respective locations.

(2) MP Check. An MP check is required for U.S. citizens before a temporary or regular installation pass may be issued.

f. *Aufenthaltstitel*. An *Aufenthaltstitel* is not required for individuals in this category.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring IRG. The sponsoring IRG may impose further restrictions. Access may be extended to the DRG only if the DRG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. The sponsoring USAG will determine restrictions on when access may be granted.

i. Restrictions on Sign-In Privileges. Individuals in this category are not authorized sign-in privileges.

j. FPCON Restrictions. During heightened FPCON levels, access to installations is restricted to FPCON Bravo.

SECTION IV
INSTALLATION PASS

29. APPLICATION PROCESS

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

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

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

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

(4) To extend a temporary installation pass.

b. IACS registrars will review the application and supporting documents and reject any application that is not complete. IACS registrars will also clarify any justification that is insufficient.

c. Key components of the application process include the following:

(1) Sponsoring Organization. The sponsoring organization will designate individuals in its organization to carry out sponsoring-organization responsibilities. The sponsoring organization for each applicant is based on the applicant's category (paras 12 through 28). For example, the USAG will serve as the sponsoring organization for some applicants; the hiring organization will serve as the sponsoring organization for other applicants.

(2) Sponsoring Official.

(a) The sponsoring official is key to the integrity of the Installation Access Control Program.

(b) The commander or first lieutenant colonel or NSPS civilian equivalent in the chain of command of an organization that sponsors installation-pass applicants will designate sponsoring officials in writing. If the sponsoring organization does not have this military or civilian pay-grade structure (for example, military banking facilities or Government travel agency), the local senior manager or deputy of the organization is authorized to sign the designation memorandum for IRG access. Sponsoring organizations will update the sponsoring official designation memorandum (fig 2) annually and forward to the servicing IACO. The IACO will—

1. File and maintain the memorandum.

2. Use the memorandum to verify the authorization of the sponsoring official each time an individual applies for an installation pass, verify that the appropriate organization is listed as the sponsoring organization, and reject any application signed by an unauthorized sponsoring official.

(c) Sponsoring officials must be DOD ID cardholders or full-time LN employees. The following are minimum grade requirements and limits on the sponsoring official's approving authority:

1. Supervisor who is a sergeant first class, chief warrant officer 2, GS-9 or NSPS equivalent, or C6A: authorized to sponsor individuals for only single-installation access.

2. Supervisor who is a first sergeant or master sergeant, chief warrant officer 3, captain, GS-11 or NSPS equivalent, NF 4, or C7: authorized to sponsor individuals for IRG access.

3. Supervisor who is a sergeant major, major, chief warrant officer 4 or 5, GS-12 or NSPS equivalent, NF 4, or C7A: authorized to sponsor individuals for DRG access.

LETTERHEAD

Office Symbol *Date*

MEMORANDUM FOR (*enter the name of the servicing IACO*)

SUBJECT: Designation of Sponsoring Officials

1. The following individuals are designated as sponsoring officials for (*enter the name of the organization*):

a. Authorized to grant up to Army-in-Europe-wide access (*minimum LTC/GS-13* (*or NSPS civilian equivalent*)*/C8/NF 5*):

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

b. Authorized to grant up to DRG-wide access (*minimum CSM/SGM/MAJ/CW4/GS-12* (*or NSPS equivalent*)*/C7A/NF 4*):

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

Figure 2. Format for Designating Sponsoring Officials

c. Authorized to grant up to IRG-wide access (*minimum 1SG/MSG/CW3/CPT/GS-11* (*or NSPS equivalent*)/*C7/NF 4*):

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

d. Authorized to grant access for only one installation (*minimum SFC/CW2/GS-9* (*or NSPS equivalent*)*/ C6A*):

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

2. The POC for this information is (*include name, telephone number, and e-mail address*).

Signature block of commander
or designated official
(*commander or first LTC/*
GS-13 (*or NSPS equivalent*)
in the chain of command)

Figure 2. Format for Designating Sponsoring Officials—Continued

4. Supervisor who is a lieutenant colonel, GS-13 or NSPS civilian employee equivalent, NF 5, or C8: authorized to sponsor individuals for Army-in-Europe-wide access. Paragraph 12 provides additional restrictions for applicants in the Contractor (Resident of European Union (EU) or NATO-Member Country) category.

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

(d) NATO Sending States and the United States Mission, Germany, will submit their sponsoring-official-designation memorandum to the USAREUR PM. This memorandum is valid for 1 year. The PM will post this memorandum to the restricted portion of the IACS website, where it is available to all IACOs. IACOs will honor any memorandum posted on the IACS website, regardless of the requirements in (b) and (c) above.

(e) Sponsoring officials will ensure the requirements and intent of this regulation are followed, physically review the application packet for correctness, and sign original documents with their signature (a stamp is not authorized).

(3) Category. An applicant's category will determine the type of installation pass that may be issued and the associated restrictions. Sponsoring officials will state the category on the application (block 7) and IACO registrars will verify its correctness. The registration requirements and restrictions vary among categories.

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

(5) Background Checks.

(a) Background checks are used to determine if an applicant is a security risk. Sponsoring organizations should refer to the appropriate category (paras 12 through 28) to determine the exact background-check requirements for each applicant. Sponsoring organizations are responsible for completing or initiating required background checks. IACO registrars are responsible for verifying that a background check has been completed or, when applicable, that it has been initiated. The types of background checks used for installation passes are as follows:

1. PGCC (*Polizeiliches Führungszeugnis*). The applicant will get this certificate from his or her city ordinance office (*Ordnungsamt*). The certificate is based on records available to the German Government and should have "No Record of Misconduct (*Keine Eintragung*)" stamped on the bottom. A translation must be obtained for any other annotations. Certificates that are more than 12 months old may not be used. If an individual is unable to get a German PGCC (for example, if he or she has less than 1 year of residency in Germany), a PGCC equivalent is required from the previous country of residence and it must be translated into English and notarized.

2. MP Check. MP checks apply only to U.S. citizens. Sponsoring officials will obtain an MP check from their servicing MP station.

3. LNSP. Sponsoring organizations will comply with LNSP procedures in AE Regulation 604-1. Registrars will log on to the LNSP website (*https://www2.dcsg2.hqusareur.army.mil/FNSPdb/login.aspx?ReturnURl=%2fFNSPdb%2fdefault.aspx*) to confirm LNSP background-check initiation and completion. Questions about the LNSP should be addressed to the unit or organization security officer.

a. Sponsoring officials will notify the IACO either in person or by e-mail where the temporary installation pass was issued when the LNSP background check is complete.

b. When the LNSP is complete (without entries), the applicant must return the temporary installation pass in order to obtain a regular installation pass.

NOTE: An individual must have lived in Germany during the past 12 or more months for an LNSP background check to be initiated. The signed AE Form 604-1B need not be turned in to the IACO as part of the application packet.

(b) Background checks that uncover no derogatory information are forwarded to the sponsoring organization.

(c) Background checks that uncover derogatory or adverse information will be forwarded to the sponsoring organization and to the host DRG. The DRG will use the commanders' adjudication policy based on the Presidential Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (at *http://www.rjhresearch.com/ADR/index.htm*) to coordinate with the sponsoring organization to determine whether the information warrants denial of access privileges. If the requested access is for more than one DRG and the DRG commander recommends the applicant for approval, the USAREUR PM will adjudicate the applicant's installation-pass request. Adjudication packages submitted to the USAREUR PM must include the DRG commander approval memorandum, AE Form 190-16A, LNSP and PGCC reports, and any memorandums by the applicant and his or her supervisor.

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

2. If the DRG commander-supported applicant is denied an Army-in-Europe-wide installation pass by the USAREUR PM based on an adverse background check, the DRG commander can assume the potential risk and may issue an installation pass for only his or her DRG.

(d) If the 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. If the applicant is not a German resident, require the applicant to provide his or her country's equivalent of the PGCC and require this document to be translated into English and notarized.

2. More closely scrutinize access requirements and limit the number of installations and times when access is allowed.

3. If the category allows sign-in privileges, deny these privileges to anyone who cannot provide adequate background-check information.

4. Limit the duration of the installation pass to coincide with the date when the individual will have 12 months of residency in Germany and an LNSP background check can be conducted.

(6) *Aufenthaltstitel* for Germany.

NOTE: USAGs in Belgium, Italy, and the Netherlands will follow the USAG guidance on residence and work permits.

(a) Citizens of the following EU countries do not require permits to reside or work in Germany: Austria, Belgium, Cyprus (Greek Part), Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

(b) Citizens of the following EU countries citizens do not require residence permits but are required to have an EU work permit (*Arbeitserlaubnis-EU*) authorizing them to work in Germany: Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia.

(c) German labor agencies stopped issuing separate residence and work permits on 31 December 2004. Separate permits will remain in effect during the transition period, but will eventually be replaced. In place of separate residence and work permits, individuals will be issued a "residence certificate" (*Aufenthaltstitel*) that may be either a temporary residence and work permit (*Aufenthaltserlaubnis zu Erwerbszwecken*) or a permanent combined residence and work permit (*Niederlassungserlaubnis*). Both the *Aufenthaltserlaubnis* and *Niederlassungserlaubnis* are acceptable documents for issuing an installation pass. It is also possible to have a residence certificate (*Aufenthaltstitel*) that does not grant employment rights to the individual. The residence certificate should be easily distinguishable as an *Aufenthaltserlaubnis* or a *Niederlassungserlaubnis* in order to be used to gain employment and an installation pass.

(7) Limit Access to Minimum Number of Installations. 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 to which access is required by listing the specific names of the installations (for example, Taylor Barracks and Coleman Barracks).

(b) If greater access is required, additional documentation is required, such as a contract statement of work.

(8) Limit Access to Minimum Days and Times. The individual's sponsoring official must review the installation-access requirement and limit it to the minimum number of days and times.

(9) Sign-in Privileges. This justification must not be based only on convenience for the installation-pass holder or sponsoring organization and it must clearly explain why the installation-pass holder requires sign-in privileges. In most cases, sign-in privileges are limited to other contractors and individuals on official business, not for personal business.

(a) IACO registrars will ensure the military and civilian grade requirements of the sponsoring official are met when sign-in privileges are requested for contractors in the Contractor (Resident of European Union (EU) or NATO-Member Country) category (para 12i).

(b) Sign-in privileges are not authorized for temporary installation-pass holders.

(c) An authorized individual can sign in up to four individuals and their vehicles.

(10) FPCON Restrictions. FPCON restrictions are based on an individual's category and function (essential or first-responder). The IACS prohibits access beyond the FPCON associated with the category (paras 12 through 28). For access during FPCON Charlie, the sponsor must state the essential functions (glossary) that must be performed. For access during FPCON Delta, the sponsor must state the "First-Responder" functions (for example, performs fire, medical, critical mechanical, electrical, and water functions or other critical functions).

(11) State Sponsors of Terrorism. Citizens from countries identified by the United States Department of State (*http://travel.state.gov/visa/temp/info/info_1300.html*) require USAG commander approval for USAG access, and USAG commander and USAREUR PM approval for Army-in-Europe-wide access. The United States Department of State requires additional screening for citizens from identified countries before they are granted entry into the United States (Immigration and Nationality Act (8 USS. 1101(a)(15) and Section 306 of the Enhanced Border Security and Visa Reform Act of 2002). Citizens from countries identified by the United States Department of State as state sponsors of terrorism who have previously been issued an installation pass are exempt from the requirement to obtain USAG commander's approval for access.

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

d. When the application is complete, the sponsoring official will escort the applicant to the servicing IACO with the required documentation (e below). If the sponsoring official cannot escort the applicant and the applicant has no other means of obtaining access to the installation, the following procedures are authorized:

(1) The sponsoring official will send the application by e-mail to the servicing IACO and inform the issuing official of the approximate date and time the applicant will come to the installation.

(2) The IACO issuing official will verify that the e-mail message is from an authorized sponsoring official by checking the memorandum designating sponsoring officials from the sponsoring organization.

(3) When the applicant arrives at the ACP, the guard will call the IACO to verify that the applicant is expected and that the IACO has received an e-mail from the sponsoring organization.

(4) The guard will check the applicant's passport or personal ID card (whichever is listed in the signed application that the applicant must have in his or her possession) and grant the applicant unescorted access.

NOTE: Under no circumstances will the applicant obtain an installation pass from the IACO without either the sponsoring official's presence or previous coordination with the IACO.

e. Applicants will submit the following documentation with the application:

(1) A copy of one of the following:

(a) Passport.

(b) Personal ID card issued by the country of citizenship (for example, German *Personalausweis*, Belgian Identity Card, Italian *carta d'identita*).

(c) Military ID card issued by one of the NATO Sending States (Belgium, Canada, France, the Netherlands, and the United Kingdom).

(2) A copy of the results of all required background checks.

(3) Verification that the applicant has an *Aufenthaltstitel*, if required.

(4) A copy of the agreement (club membership, *in loco parentis* memorandum, AE Form 600-700A, contract) justifying the need for installation access and verification of the expiration date.

f. Before giving the applicant an installation pass, the IACS registrar will ensure that the applicant signs and dates an installation-pass holder acknowledgement of responsibilities (app C (English), app D (German)) and, for LN personnel, the *Datenschutzerklärung* statement (app E (Privacy Act)).

g. The IACS registrar will file the completed application packet. A complete application packet will include the application (AE Form 190-16A), a copy of supporting documents, a copy of the background-check initiation and results, the original copy of the acknowledgement of responsibilities memorandum, the *Print Summary Page* from the IACS, the original signed IACS installation-pass-holder consent form (AE Form 190-16E), and the signed *Datenschutzerklärung*. For temporary installation-pass holders receiving a regular installation pass, the issuing official will file the notification information with the original temporary installation-pass application packet.

(1) According to AR 25-400-2, AE Regulation 25-400-2, and the Army Records Information Management System, AE Form 190-16A is considered a "transfer" record type for U.S. citizens and must be destroyed after 5 years. For archived and expired IACS files less than 5 years old, the original AE Form 190-16A will be kept and photocopied supporting documentation will be destroyed.

(a) Files must be arranged in special-use records-shipping boxes (national stock number 8115-00-117-8249), which are available at supporting self-service supply centers or from the General Services Administration.

(b) Boxes must be shipped to the Army in Europe Records Holding Area at Panzer Kaserne in Kaiserslautern, Germany. A completed SF 135 listing box contents by name must be included in the shipment.

(2) The collection, processing, and storing of LN data must adhere to the provisions of the *Datenschutzerklärung*.

30. APPLICATION PROCEDURES FOR APPLICANTS WITH TEMPORARY INSTALLATION PASSES

a. These procedures do not require the sponsoring organization to submit a new application.

b. Sponsoring officials will notify the IACO either in person or by e-mail where the temporary installation pass was issued and when the LNSP background check was completed.

c. If the notification is by e-mail, the IACO issuing official will verify that the e-mail message is from an authorized sponsoring official by checking the memorandum designating sponsoring officials from the sponsoring organization (fig 2).

d. The IACO notification must include the date the LNSP background check was completed and that the results include no derogatory information. If derogatory information is found, the notification must state that the host DRG and sponsoring official have reviewed the results and determined that there is no derogatory information present to warrant denial of installation-access privileges. The notification will also include any other changes the sponsoring official wants to make since the temporary installation pass was issued.

e. When the notification is received, the applicant will return the temporary installation pass and obtain a regular installation pass. The notification paperwork is filed with the original temporary installation-pass application packet.

31. APPLICATION PROCEDURES TO RENEW AN INSTALLATION PASS

a. Sponsoring officials will submit a new application (AE Form 190-16A) to validate the information on the original application. Requests may be processed 45 days before the expiration date and IACOs may issue a pass 90 days after the expiration date if the individual is unavailable to renew the pass (for example, because of illness, injury, TDY).

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

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

(a) A certificate was required based on the person's category. This requirement does not apply to individuals in the Local National Employee category (para 20).

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

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

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

(4) Whenever possible, installation passes are renewed at the IACO that issued the initial installation pass in order to maintain record continuity.

c. IACOs will ensure applicants turn in their expiring or expired installation pass or the AE Form 190-16B receipt for it (if access control personnel confiscated an expired pass) before receiving a new installation pass.

NOTE: Individuals in the Local National Employee category (para 20) 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 PGCC. These transfers are documented on the new application.

32. APPLICATION PROCEDURES FOR LOST OR STOLEN PASS

If an installation pass is lost or stolen, the installation-pass holder must immediately report it 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 where the original installation pass was obtained. 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 for that individual's category. With the exception of LN employees, a new PGCC may be required if it is older than 12 months.

33. APPLICATION PROCEDURES FOR EXTENSION OF TEMPORARY PASS

a. IACOs may grant a 90-day extension to a temporary installation pass if the LNSP results are being processed and have not yet been received. If the LNSP results reveal derogatory (adverse) information, another temporary installation pass will not be issued.

b. Background checks with derogatory (adverse) information will be processed according to paragraph 29c(5)(c).

34. UNSERVICEABLE PASSES

An unserviceable installation pass may be exchanged, one-for-one, at the pass-holder's servicing IACO without action from 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 is the same as that on the original installation pass.

SECTION V
INSTALLATION ACCESS CONTROL OFFICE

35. GENERAL

a. Only USAREUR-approved IACOs are authorized to issue installation passes. A complete list of authorized IACOs is available at *http://www.hqusareur.army.mil/opm/iacs/iacs.html*.

b. Access control is an installation commander's responsibility. Organizations outside the direct control of the USAG will not be authorized to issue installation passes or equipped with IACS scanners.

c. IRGs should functionally align their IACO under their servicing director of emergency services (DES).

d. IACO registrars will—

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

(2) Develop a system to conduct reconciliation 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 the security, accountability, and procurement of installation-pass material is maintained:

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

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

36. REGISTRATION PROCEDURES FOR IDENTI-KID

Parents and legal guardians with children under the age of 10 and who do not have DOD ID cards may register their children in the IACS using an Identi-Kid kit. The Identi-Kid kit 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

37. SIGN-IN PROCEDURES

Sign-in procedures provide access to U.S. Forces installations if an access roster is unnecessary and issuing an installation pass is impractical or not authorized.

a. Sign-In Privileges.

(1) DOD ID cardholders who are 18 years old or older and military spouses under the age of 18 have sign-in privileges. If this privilege has been suspended, it is documented in the IACS and will be checked by a guard in the IACS when the DOD ID cardholder tries to use his or her sign-in privileges.

(2) Except for individuals in the NATO Member and Department of State and American Embassy Personnel categories, installation-pass holders are not granted sign-in privileges unless authorized by the sponsoring organization. Sign-in 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. The installation-pass holder must be at least 18 years old.

b. Restrictions.

(1) Temporary installation-pass holders are not authorized sign-in privileges.

(2) DOD ID cardholders not registered in the IACS are not authorized sign-in privileges. Exceptions are for active duty DOD ID cardholders who are either on TDY or leave. (For example, a DOD ID cardholder who is on leave from a deployment and visiting USAG Garmisch may sign in Family members and guests with an approved leave form.)

(3) Sign-in privileges are limited to signing in four individuals and their vehicles at any one time.

(4) Individuals who require recurring access will not use sign-in procedures to avoid the installation-pass application process or access-roster requirements.

c. FPCON Restrictions. During FPCON Charlie, host-nation contractors and official guests are not authorized sign-in privileges. During FPCON Delta, only DOD ID cardholders are authorized sign-in privileges. Exceptions may be granted by USAG commanders for key and essential personnel.

d. Identification.

(1) Individuals who are signed in must show the guard their passport or personal ID (for example, German *Personalausweis*, Belgian Identity Card, Italian *carta d'identita*). Guards will ensure through visual comparison that the passport or personal ID belongs to the person being signed in.

(2) If the ACP is equipped with IACS scanners, guards will—

(a) Open the sign-in module and scan the DOD ID card or installation pass of the individual exercising his or her sign-in privileges. The IACS automatically displays a warning message if the individual is not authorized sign-in privileges and will not allow other data to be entered.

(b) Enter the names of the individuals being signed in. The IACS automatically checks the bar roster to ensure these individuals are not barred from the installation.

(3) If the ACP is not equipped with IACS scanners, the local SOP will provide procedures for accounting for signed-in individuals.

e. Sponsor Responsibilities. Sponsors will ensure any individuals they sign in are physically escorted at all times. Failure to follow this policy may lead to administrative actions such as suspension or revocation of the sponsor's sign-in privileges and installation access.

38. ACCESS ROSTERS

a. Access rosters are used to provide access to installations if sign-in procedures and issuing an installation pass are impractical or unauthorized.

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 60 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 can be used for individuals with a current PGCC (within the last 12 months) identified as temporary hires (up to 60 days). Temporary hires are individuals who do not have permanent employment requiring recurring and regularly scheduled work, but are on call to substitute for a permanent employee.

e. Individuals with a current PGCC 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 who is on call to fix playground equipment).

f. Individuals with an adverse PGCC or LNSP check that has not been adjudicated may not be placed on an access roster.

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

Example 1: An authorized DOD ID cardholder requires four meetings with several LN personnel (not associated with the U.S. Armed Forces) over a 3-week period to discuss a project affecting the host nation. An access roster would be appropriate for LN personnel because the meetings are not regularly scheduled, are site-specific, and are not scheduled beyond 60 days.

Example 2: A sanctioned private organization (for example, dance club) meets every Wednesday evening at 1900 and several of the members are LN employees. An access roster is not appropriate because the meetings are a recurring event. The participants must be signed in each week or issued an installation pass based on the Member of Private Organization category (para 21).

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.

Example 4: A DOD ID cardholder wants to host a surprise birthday party at a Family and morale, welfare, and recreation facility and the guest list includes 10 people 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 registered in the IACS may sign an access-roster request (AE Form 190-16F). IACO registrars will check the IACS to ensure the requester is a registered DOD ID cardholder.

(2) Original access-roster requests must be hand-carried to the servicing IACO or sent from an official e-mail address (for example, .aafes.com, .eu.dodea.edu, .gov, .mil, .nato, .org). If the request is sent by e-mail, the IACO issuing official will confirm receipt. Access-roster requests may not be sent by fax.

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

(4) Access rosters must include the following information:

(a) Full name, country of citizenship, passport number or personal ID number (the number from one of the documents listed in paragraph 29e, which must be shown to the guard before access is granted), and vehicle license-plate number, if applicable, of each individual.

(b) An effective date and expiration date (no more than 60 days).

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

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

(e) If the access roster is being used to support nonrecurring delivery services, the days and times when deliveries may be made (for example, Mondays from 0700 to 1600).

(f) 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 contracted delivery services), a PGCC is required and rules concerning the requirements for an *Aufenthaltstitel* apply. Personnel who do not live in Germany will need to provide their country's equivalent of the PGCC, translated into English and notarized. This documentation must accompany the access-roster request. If the request is sent by e-mail, the requester must include a scanned copy of all required documentation.

(5) If an access roster is limited to one installation, the IRG may allow the access roster to be processed through designated individuals representing that installation (for example, the installation coordinator). IRGs will ensure these procedures are in local SOPs and special orders for ACP guards.

(6) IRGs will establish procedures to ensure—

(a) Individuals on access-roster requests are screened against bar rosters, and their country of citizenship is checked to ensure that any residence- and work-permit requirement is met.

(b) Access rosters are clearly marked to indicate they have been approved by the IRG before distribution.

(c) Approved access rosters are posted at applicable ACPs before the effective date.

i. If the IACS is not operational at USAG ACPs, access-control guards will do the following:

(1) When an individual arrives at an ACP and informs the guard that he or she is on an access roster, the guard will obtain the individual's passport or personal ID and check the numbers by seeing if they are listed on the access roster.

(2) Guards will deny access when an individual is not on the access roster, information on the passport or personal ID card is not consistent with the information on the access roster, or the access roster has expired.

(3) If the access roster is being used to support delivery requirements, guards will check delivery paperwork to ensure the delivery location is identified.

(4) When access is authorized, guards will search the individual, bags, and vehicles according to the local SOP.

j. When the IACS is operational at USAG ACPs, the USAG will use the access-roster module in the IACS to process access rosters.

(1) IACO registrars will enter the access-roster information into the IACS and keep a printed copy of the access-roster request for distribution as needed.

(2) Guards will follow the procedures in subparagraph i above, except that they will conduct a manual lookup in the IACS instead of using a printed access roster.

39. EMERGENCY-VEHICLE ACCESS

a. Access During Emergencies.

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

(2) In situations where the host-nation 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.

(3) Ambulance service is provided by host-nation hospitals. Ambulances in Germany are well-marked with some or all of the following words: Ambulance, *Krankenwagen, Rettungswagen*, or *Notarzt*. USAGs in Belgium, Italy, and the Netherlands should include a description of the host-nation ambulances in their local SOPs.

b. Host-Nation Police.

(1) When on routine patrol or investigative duty, host-nation police and MP are required to present their official ID when entering U.S. installations, even if they are in marked police vehicles and wearing host-nation police uniforms. The German Police ID or *Polizeidienstausweis* is different for each State or Federal police force (for example, *Bundeskriminalamt* or *Bundespolizei*), but is a paper or plastic card with the name and picture of the officer on it and his or her registration number. German MP vehicles are marked *Feldjäger* and German MP personnel carry a *Truppenausweis* (military ID card). German customs investigators carry a *Dienstausweis* that has the name and picture of the officer on it and his or her registration number, and is issued by the respective customs office. USAGs in Belgium, Bulgaria, Italy, and the Netherlands should include a description of the host-nation police IDs in local SOPs. If there is any reason to doubt the validity of an ID or the reason for entry onto an installation, the guard will call the servicing U.S. Forces police (for example, MP).

(2) Host-nation police who work on an installation with the U.S. Forces police may be issued an installation pass using the Official Guest category (para 23) to access the installation.

c. Other Host-Nation Providers. IRGs should develop alternate access-control procedures for other host-nation service providers that respond to emergencies that are not life-threatening (for example, water-, electric-, and heating-service providers). In these situations, unimpeded access should not be granted. IRGs should develop memorandums of agreement that require these service providers to notify the installation ahead of time when access is required.

40. 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 did not occur, only HAV drivers must present their DOD ID card (no dispatch, license, or other documents). Exceptions to this requirement are on an installation basis and approved by the DRG commander. Other occupants in HAVs will not be asked to provide ID.

(4) Guards will request that only the driver's window be opened to receive the driver's ID card. The 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 first (lead) HAV driver 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 prudent security procedures.

b. Arms-Control Treaty Vehicles.

(1) The primary treaties to which U.S. organizations in Europe are subject include the Conventional Forces, Europe; the Vienna Document 1999; and the Treaty on Open Skies. According to AE Regulation 525-50, the treaty compliance officer will notify the USAG of an inspection and coordinate access for teams conducting treaty compliance inspections under these and other treaties. Such teams will arrive at U.S. installations under escort in vehicles provided by the host nation.

NOTE: Host-nation security personnel will search vehicles used to transport inspection teams before their arrival at the installation. The inspectors and the property under their control are screened and cleared during "point of entry" procedures as specified by the treaty. During treaty inspections, inspectors operate under diplomatic immunity and consequently may not be searched again by gate guards or other military law-enforcement or security personnel.

(2) When a treaty inspection or exercise occurs, the gate guard will follow the instructions of the site commander and the treaty compliance officer to allow access for treaty vehicles.

41. ACP GUARDS

a. ACP guards will—

(1) Perform their duties according to this regulation and AE Regulation 190-13.

(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 40. Table 1 lists the appropriate actions for scanned responses from the handheld scanner.

Table 1
Guard Actions for Scanned Responses From Handheld Scanners

Main Message	Supporting Message	Description	Action
STOP	BARRED	This person's record has been flagged as "barred" in the DBIDS-IACS database.	Do not allow on installation. Detain individual and vehicle, and call law-enforcement officials. **DOD ID Card:** If the card has expired, confiscate and issue AE Form 190-16B to the individual. **Installation Pass:** Confiscate and issue AE Form 190-16B to the individual.
STOP	CALL LAW ENFORCEMENT	This person's record has been flagged as "call law enforcement" in the DBIDS-IACS database.	Detain 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 ACP is operational, allow on the installation.	Detain individual and vehicle and call law-enforcement officials for instructions listed in the "Remarks" section of the IACS LEO module lookup "Search IACS Registered Persons Records." **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 on the installation and instruct the individual to proceed to the IACS office to correct the problems with his or her ID card. **Installation Pass:** If there are no instructions, do not allow on 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 on 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 on installation and instruct the individual to proceed to the IACS office 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 on installation.
STOP	ACCESS DENIED TO THIS INSTALLATION	This person has an active DBIDS-IACS record, but is not allowed access to this installation.	Do not allow on installation without additional documentation (TDY or other official orders specifying this installation) or when a "Visitor Category" and installation-pass holder is accompanied by a DOD ID cardholder.
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.	Do not allow on installation without additional documentation (TDY or other official orders specifying this installation) or when a "Visitor Category" and installation-pass holder is accompanied by a DOD ID cardholder.

Table 1
Guard Actions for Scanned Responses From Handheld Scanners

Main Message	Supporting Message	Description	Action
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.	Do not allow on installation without additional documentation (TDY or other official orders specifying this installation) or when a "Visitor Category" and installation-pass holder is accompanied by a DOD ID cardholder.
STOP	ID CARD EXPIRED	ID card is no longer valid.	Allow on installation but confiscate the ID card or installation 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 on installation and instruct the individual to proceed to the IACS office 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 41e and f. Try to verify the person's registration in the IACS laptop using manual lookup. If registered, allow on 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 into IACS. Allow on installation and instruct the individual to proceed to the IACS office to correct the problems with the ID card. **Installation Pass:** If not registered, do not allow on the installation, confiscate the pass, and issue AE Form 190-16B to the individual. If an ID card or an installation pass appears to have been tampered with, confiscate and issue AE Form 190-16B to the individual, detain the individual, and call law-enforcement officials.
STOP	UNABLE TO DECODE ID CARD	The Symbol 2846 Handheld could not recognize the Code 39 barcode as one that is maintained by the DBIDS-IACS.	Follow the guidance in paragraphs 41e and f. Try to verify the person's registration in the IACS laptop. If registered, allow on 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 into IACS. Allow on installation, and instruct the individual to proceed to the IACS office to correct the problems with his or her ID card. **Installation Pass:** If not registered, do not allow on the installation, confiscate the pass, and issue AE Form 190-16B to the individual. If an ID card or an installation pass appears to have been tampered with, confiscate the card and 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.	**DOD ID Card:** Ask for a second form of photo ID and supporting documentation, such as TDY orders or a leave request. Log into IACS. Allow on the installation, and instruct the individual to proceed to the IACS office to register his or her ID card in the IACS.

Table 1 Guard Actions for Scanned Responses From Handheld Scanners			
Main Message	**Supporting Message**	**Description**	**Action**
		NOTE: If the DOD ID card or installation pass was recently entered into IACS (within the last 24 hours) and the IACS ACP is operational, allow on the installation.	**Installation Pass:** Do not allow on the installation, confiscate the pass, and issue AE Form 190-16B to the individual.

NOTE: The IACS LEO module located at the law-enforcement desk is used to determine actions for flagged IACS records.

(3) Follow the sign-in policy and procedures in paragraph 37 and the access-roster policy and procedures in paragraph 38.

NOTE: All personnel conducting access control may confiscate DOD ID cards or installation passes using AE Form 190-16B. In accordance with paragraph 5h(1)(b), the USAG will establish receipt procedures for individuals whose cards or passes are confiscated and procedures to ensure these documents are turned in to the servicing IACO or ID-card-issuing facility as appropriate. A receipt for confiscated or expired DOD ID cards or installation passes will not be used as an authorized access document.

b. If the IACS is unavailable, guards will manually check access documents. A second form of photo ID and a vehicle registration may be required based on local policy (for example, thoroughly checking personnel and vehicles during a specific FPCON or random antiterrorism measure). USAGs will include procedures for manually checking access documents in USAG policy and SOPs.

c. When the IACS is operational at an ACP, guards will scan 100 percent of DOD ID cards and installation passes unless operational requirements temporarily force the use of manual procedures to augment the IACS.

d. If scanning reveals that an installation-pass holder or DOD ID cardholder is not registered in the IACS and the pass 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 IACS, the guard will—

(1) Ask for a second form of photo ID.

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

NOTE: If the individual does not have a second form of photo ID, the guard will deny access. The DOD ID card or CAC cannot be validated.

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

f. If a DOD ID cardholder or installation-pass holder has forgotten his or her card or pass, guards will use the IACS manual look-up feature at the ACP to authorize and record access.

g. Normally a contract security guard is issued an installation pass in the Gate Guard category (para 17). If the contract security guard has additional installation-access requirements based on his or her position or duty location, he or she may apply for an installation pass using the Contractor (Resident of European Union (EU) or NATO-Member Country) category (para 22).

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

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

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

Public Law 106-246, Military Construction Appropriations Act, 2001

Privacy Act of 1974

United States Code, Title 5, section 552, Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

United States Code, Title 10, section 3013, Secretary of the Army

United States Code, Title 10, section 5013, Secretary of the Navy

United States Code, Title 10, section 8013, Secretary of the Air Force

DOD Directive 8500.01E, Information Assurance (IA)

AR 25-2, Information Assurance

AR 190-13, The Army Physical Security Program

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

AR 381-45, Investigative Records Repository

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

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

AE Regulation 190-13, Army in Europe 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 715-9, Contractor Personnel in Germany—Technical Expert, Troop Care, and Analytical Support Personnel

SECTION II
FORMS

SF 50-B, Notification of Personnel Action

SF 135, Records Transmittal and Receipt

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

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

DD Form 2(RES), Armed Forces of the United States Geneva Convention Identification Card (Reserve)

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

DD Form 577, Appointment/Termination Record - Authorized Signature

DD Form 1172, Application for Uniformed Services Identification Card—DEERS Enrollment

DD Form 1173, United States Uniform Services Identification and Privilege Card (Dependent)

DD Form 1173-1, United States Uniformed Services Identification and Privilege Card (Reserve Dependent)

DD Form 1934, Geneva Convention 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

DA Form 31, Request and Authority for Leave

DA Form 2028, Recommended Changes to Publications and Blank Forms

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

AE Form 190-16A, Application for U.S. Forces in Europe Installation Pass

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

AE Form 190-16C, Record of Destruction

AE Form 190-16E, IACS Installation-Pass-Holder Consent Form

AE Form 190-16F, Installation Access Control System (IACS) Access-Roster Request

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

APPENDIX B
HEIGHT AND WEIGHT CONVERSION CHARTS

Weight-Conversion Chart			Height-Conversion Chart		
(2.2045 pounds = 1 kg)			(.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-PASS HOLDER ACKNOWLEDGEMENT OF RESPONSIBILITIES (ENGLISH)

Installation-Pass Holder Acknowledgement of Responsibilities

1. As a U.S. Forces in Europe installation-pass holder, I acknowledge the following:

a. All persons, their personal property, U.S. Government property, and vehicles may be searched on entry, while within the confines of, or when leaving U.S. Forces installations. Persons trying to enter who refuse to identify themselves, provide digitized fingerprint data, or consent to being searched will be denied access.

b. If I am authorized sign-in privileges, I understand that at no time will I have more than four persons and their vehicles signed in. I understand that by signing for another person to enter a U.S. Forces installation, I am agreeing to monitor that person's actions at all times, and I accept full responsibility for that person's conduct. I will ensure that the signed-in person complies with U.S.-Forces and local policy.

c. Installation passes are U.S. Government property. Any access-control person may confiscate an installation pass that has expired, is being used fraudulently, is being presented by a person other than the person to whom it was issued, or is obviously altered, damaged, or mutilated.

d. I must surrender my pass when any of the following occurs:

(1) The pass is replaced (except when lost or stolen).

(2) I no longer require access.

(3) My sponsor status changes.

(4) I resign or retire, am terminated, or am no longer officially sponsored.

e. If I lose my installation pass or if it is stolen, I must immediately notify either the military police or installation access control office that issued the pass. Failure to do so is grounds for denying a replacement pass.

f. Violations of U.S. Forces security policy may be grounds for denying access to U.S. Forces installations and lead to confiscation of installation-access documents.

2. I acknowledge by my signature that I have read and understand the above policy, requirements, and responsibilities.

_____	_____	_____
Last, First, MI (Print)	Signature	Date

APPENDIX D
INSTALLATION-PASS HOLDER ACKNOWLEDGEMENT OF RESPONSIBILITIES (GERMAN)

Anerkennung der Pflichten eines Ausweisinhabers

1. Als Inhaber eines Kasernenausweises von *U.S. Forces* erkenne ich Folgendes an:

a. Alle Personen sowie sämtliche mitgeführten Gegenstände (persönliche Gegenstände wie auch im Eigentum der US-Regierung befindliche Gegenstände) und Kraftfahrzeuge können beim Betreten von bzw. bei der Einfahrt in Einrichtungen der US-Streitkräfte, während des Aufenthaltes in diesen Einrichtungen oder beim Verlassen der Einrichtungen durchsucht werden. Personen, die versuchen, Zugang zu einer Einrichtung zu erhalten, sich aber weigern sich auszuweisen, sich digitale Fingerabdrücke abnehmen oder sich, Gegenstände und Fahrzeuge durchsuchen zu lassen, kann der Zugang verweigert werden.

b. Erhalte ich die Berechtigung, Personen in Besucherlisten einzutragen, so bin ich mir bewusst, dass ich zu keinem Zeitpunkt mehr als vier Personen und deren Fahrzeuge eintragen darf. Ich bin mir auch bewusst, dass ich mich mit dem Eintragen anderer in Besucherlisten verpflichte, deren Handlungen jederzeit zu überwachen und für ihr Verhalten die volle Verantwortung zu übernehmen. Ich werde sicherstellen, dass die eingetragenen Personen Bestimmungen der US-Streitkräfte sowie örtlich geltende Bestimmungen einhalten.

c. Kasernenausweise sind Eigentum der US-Regierung. Zugangskontrollpersonal kann abgelaufene Ausweise sowie Ausweise, die in betrügerischer Weise verwendet oder von Personen vorgelegt werden, auf die sie nicht ausgestellt sind, einziehen. Das Gleiche gilt für Ausweise, an denen offensichtlich Veränderungen vorgenommen wurden, die beschädigt oder zerschnitten sind.

d. Ich habe meinen Kasernenausweis abzugeben, wenn

(1) er durch einen anderen ersetzt wird (Ausnahme: gestohlene bzw. abhanden gekommene Ausweise);

(2) ich nicht länger Zugang zu Einrichtungen benötige;

(3) sich mein *Sponsor*-Status ändert;

(4) ich aus dem Dienst ausscheide, in den Ruhestand gehe, gekündigt werde oder nicht länger einen offiziellen *Sponsor* habe.

e. Bei Verlust und Diebstahl meines Kasernenausweises habe ich umgehend die US-Militärpolizei bzw. das *Installation Access Control Office*, das den Ausweis ausstellte, zu benachrichtigen. Bei Nichtanzeige kann die Ausstellung eines Ersatzausweises verweigert werden.

f. Bei Verstößen gegen Sicherheitsbestimmungen der US-Streitkräfte kann mir der Zugang zu deren Einrichtungen verweigert oder die Zugangsberechtigung entzogen werden.

2. Mit meiner Unterschrift bestätige ich, dass ich vorstehenden Bestimmungen, Vorgaben und Pflichten zur Kenntnis genommen und verstanden habe.

_____	_____	_____
Nachname, Vorname(n) (in Druckbuchstaben)	Unterschrift	Datum

APPENDIX E
CONSENT TO COLLECT PERSONAL DATA

DATENSCHUTZERKLÄRUNG

Die Regierung der Vereinigten Staaten von Amerika sieht sich in besonderer Weise dem Schutz der Privatsphäre des Individuums verpflichtet. Als Teil der Exekutive achtet das US-Verteidigungsministerium auf den Schutz persönlicher Daten, die im Rahmen dienstlicher Belange von Mitarbeitern,Vertragsnehmern und dritten Personen erhoben werden müssen. Dabei wenden die Dienststellen des Verteidigungsministeriums im Ausland das jeweils einschlägige nationale Datenschutzrecht an.

Im Hinblick auf die Bedrohung durch den internationalen Terrorismus sind die Dienststellen der US Streitkräfte bemüht den grösstmöglichen Schutz von Personal, Gerätschaften und Liegenschaften vor Anschlägen sicherzustellen. Hierzu ist es erforderlich, den Zugang zu den Liegenschaften zu beschränken und sicherzustellen dass nur berechtigte Personen Zugang erhalten. Diesem Zweck dient die Einführung eines mit biometrischen Daten (digitalisiertes Lichtbild und zwei Fingerabdrücke) ausgestatteten Ausweises, der Installation Access System Control Card, der eine schnelle und sichere Personenidentitätsfeststellung ermöglicht.

Ihre mit dem Antragsformular 190-16A zu den Nummern 4-10,13-25 erhobenen persönlichen Daten werden in eine regionale Datenbank des Installation Access Systems (IACS) aufgenommen und gespeichert. Dies gilt auch für die digitalisierten Fingerabdrücke und das Lichtbild. Für die Datenbank ist das Office of the Provost Marshal verantwortlich.

Die Daten werden ausschliesslich zur Identitätsüberprüfung im Zusammenhang mit dem Zugang zu und dem Aufenthalt in Einrichtungen der US Streitkräfte verwendet. Sie werden durch Zugangskontrollsysteme entsprechend dem jeweiligen Stand der Technik gegen unberechtigten Zugriff geschützt und sind nur dem mit der Aufgabe des Liegenschaftsschutzes betrauten Personenkreis zugänglich. Durch die Lesegeräte wird über einen automatischen Abgleich der auf dem Ausweis veschlüsselt enthaltenen Daten mit der Datenbank die Echtheit des Ausweises überprüft.

Eine Übermittlung der Daten an Stellen ausserhalb der Bundesrepublik Deutschland erfolgt nicht. Mit dem Liegenschaftsschutz betraute Dienststellen des US-Verteidigungsministeriums in Europa haben zu Zwecken der Personenzugangskontrolle Zugriff auf die gespeicherten Daten, wenn die betroffene Person eine in Europa ausgestellte Installation Access Control Card vorlegt. Eine Übermittlung von Daten an Dienststellen der Bundesrepublik Deutschland erfolgt nur soweit dies nach den rechtlichen Bestimmungen des Bundesdatenschutzgesetzes zulässig ist.

Bei einem Ausscheiden aus dem Dienst bei den US Streikräften bzw. bei Wegfall der Notwendigkeit, im Rahmen dienstlicher oder vertraglicher Belange Liegenschaften der US Streitkräfte zu betreten, werden die gespeicherten Daten in ein gesichertes Datenarchiv transferiert und dort nach Ablauf eines Zeitraums von 5 Jahren vollends gelöscht.

Andere als die mit der Antragsstellung angeforderten persönlichen Daten werden nicht erhoben. Der Antragsteller ist befugt beim zuständigen IACS-Office unentgeltlich Auskunft über die über ihn gespeicherten Daten und gegebenenfalls deren Korrektur zu verlangen.

Die Hauptbetriebsvertetung der bei den US-Armee beschäftigten Ortskräfte hat der Erhebung, Speicherung und Verwendung der persönlichen Daten im Zusammenhang mit der Einführung des neuen Liegenschaftzugangkontrollsystems zugestimmt.

Von der vorstehenden Datenschutzerklärung habe ich Kenntnis genommen. Mir ist bekannt, dass eine Verweigerung der Einwilligung zur Speicherung und Verwendung der erhobenen Daten zur Verweigerung des Zugangs zu den Liegenschaften führen kann. Dies kann – mit weiteren Folgen – dazu führen, dass ich meinen vertraglichen Verpflichtungen nicht nachkommen kann.

Ich stimme der Speicherung und Verwendung meiner Daten in der IACS Datenbank zu.

_____ _____

(Ort, Datum) (Unterschrift)

GLOSSARY

SECTION I
ABBREVIATIONS

7th CSC	7th Civilian Support Command
AAFES-Eur	Army and Air Force Exchange Service, Europe
ACP	access-control point
AOR	area of responsibility
CAC	common access card
COR	contracting officer's representative
CNE-C6F	Commander, U.S. Naval Forces Europe/Commander, U.S. Sixth Fleet
CPF	central processing facility
DBIDS	Defense Biometric Identification System
DCG, USAREUR	Deputy Commanding General, United States Army Europe
DECA-Eur	Defense Commissary Agency, Europe
DEERS	Defense Enrollment Eligibility Reporting System
DEROS	date eligible for return from overseas
DES	director of emergency services
DFMD	digitized fingerprint minutia data
DOD	Department of Defense
DODDS-Europe	Department of Defense Dependents Schools - Europe
DRG	direct-report garrison
EU	European Union
FMWR	Family and morale, welfare, and recreation
FPCON	force protection condition
G2	Deputy Chief of Staff, G2, United States Army Europe
HAV	heavy armored vehicle
HQ USAREUR	Headquarters, United States Army Europe
IACO	installation access control office
IACS	Installation Access Control System
ID	identification
IMCOM	United States Army Installation Management Command
IMCOM-Europe	United States Army Installation Management Command, Europe Region
IRG	indirect-report garrison
JA	Judge Advocate, United States Army Europe
LEO	Law Enforcement Official (Installation Access Control System module)
LN	local national
LNSP	Local National Screening Program
MI	middle initial
MIPR	military interdepartmental purchase request
MP	military police
NAF	nonappropriated fund
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NSPS	National Security Personnel System
PGCC	Police Good Conduct Certificate
PIN	personal identification number
PM	Provost Marshal, United States Army Europe

POC	point of contact
POV	privately owned vehicle
PR&C	purchase request and commitment
SCOR	site contracting officer's representative
SEV	security-escort vehicle
SF	standard form
SOFA	Status of Forces Agreement
SOP	standing operating procedure
SSN	social security number
TDY	temporary duty
TM	technical manual
TV AL II	*Tarifvertrag vom 16. Dezember 1966 für die Arbeitnehmer bei den Stationierungsstreitkräften im Gebiet der Bundesrepublik Deutschland*
U.S.	United States
USAFE	United States Air Forces in Europe
USAREUR	United States Army Europe
U.S.C.	United States Code

SECTION II
TERMS

access roster
One of four ways an individual can be granted access to U.S. Forces-controlled installations; an approved list of individuals authorized unescorted access to an installation.

applicant
An individual applying for an installation pass.

application
AE Form 190-16A used to apply for an installation pass.

category
Designation of individuals registered in the Installation Access Control System. There are 18 different categories. Each category has specific risk-based registration requirements and restrictions based on the relationship between the individual and the U.S. Forces. One category is for DOD ID cardholders; the remaining 17 categories are for installation-pass applicants.

contractor
An individual working under contract for 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.

Datenschutzerklärung
The German version of the Privacy Act Statement.

essential function
A function that if not performed would seriously affect the 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-responder
Personnel who are authorized access to an installation during force protection condition Delta because of the services they provide.

in loco parentis
In the position or place of a parent.

installation access control office
An office, normally at a United States Army garrison, that is authorized by the Provost Marshal, USAREUR, to register individuals in the Installation Access Control System and produce and issue installation passes.

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 program managed by the USAREUR G2 that is designed to conduct background checks on local national personnel and German residents.

logical access
The right to use installation-access verification systems (computers) with no right to physical access to the installation.

probable cause
Reasonable grounds for supporting that a charge is well-founded.

registrar
An official who is authorized to register individuals in the Installation Access Control System and issue installation passes. Registrars normally work at the installation access control office.

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 (para 24) and the two Visitor (paras 26 and 27) categories of the Installation Access Control System.

sign-in privileges
Privileges granted to certain categories of individuals that allows them to escort visitors after signing them onto an installation.

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

sponsoring organization
The organization that performs installation-pass responsibilities based on the organization's relationship to the installation-pass applicant. Sponsoring organizations are identified for each category of applicant. Sponsoring organizations verify the legitimacy of the applicant's need to gain access to U.S. Forces installations. Every installation-pass applicant and installation-pass holder has a sponsoring organization.

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