

19 October 2003

Military Police

Installation-Access Control

***This regulation supersedes AE Regulation 190-16, 5 December 2002.
This regulation rescinds AE Form 190-13A, Permanent U.S. Army, Europe, Installation Pass;
AE Form 190-13B, Application for Permanent U.S. Army, Europe, Installation Pass; and
AE Form 190-13C, Temporary U.S. Army, Europe, Installation Pass.**

The English version of this regulation is the governing directive.

For the CG, USAREUR/7A:

MICHAEL L. DODSON
*Lieutenant General, USA
Deputy Commanding General/
Chief of Staff*

Official:



GARY C. MILLER
*Regional Chief Information
Officer - Europe*

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

Summary of Change. This regulation has been updated to—

- Eliminate references to the “transition period” and the old installation passes (AE Form 190-13A and AE Form 190-13C).
- Replace the term “issuing official” with “registrar” throughout.
- Clarify that vehicle registration for installation-pass applicants is only for privately owned vehicles (POVs).
- Allow area support groups (ASGs) to delegate to base support battalions (BSBs) the authority to adjudicate background checks when derogatory information is present (para 5e(3)).
- Add an ASG and BSB responsibility to perform sponsoring-organization responsibilities (paras 5e(6) and 5g(6)).
- Add as a BSB responsibility that Installation Access Control System (IACS) equipment transferred to the BSB remain dedicated to support the IACS (para 5g(5)).
- Add the requirement to list installation access control office (IACO) information on purchase requests and commitments (PR&Cs), military interdepartmental purchase requests (MIPRs), and other requests for contract support when the contract will result in contractors needing access to installations (paras 5i(3) and 5k(5)).

- Add as a sponsoring organization’s responsibility the requirement to justify access privileges (para 5k(2)).
- Add that exceptions to policy that are imbedded in the IACS software can be administered by the IACO (para 7c).
- Add documents other than temporary duty (TDY) orders that can be used with an installation pass to gain access when access is temporarily required outside the area authorized by the installation pass (para 8a(2)).
- Add sponsoring-organization guidance for people in the “Contractor (Living in Host Nation)” category when access requirements are less than USAREUR-wide but cross ASG boundaries (para 15d(2)(b)).
- Change from force protection condition (FPCON) Bravo to Charlie the highest FPCON where people in the “Contractor (Living in Host Nation)” are allowed to sign in people (para 15i).
- Add that the Temporary Installation Pass is only valid at FPCONs Alpha and Bravo for people in the “Contractor (Living in Host Nation)” category (para 15j).
- Add the ability for the IACO to grant a one-FPCON exception-to-policy increase for all person categories where there is an FPCON limit.
- Add a new person category of “Host-Nation Military Member” (para 20).
- Enable persons in the “Vendor or Commercial Solicitor” category to obtain USAREUR-wide access (paras 18d and 18g).
- Add a requirement for a residence permit for applicants in the “Visitor (Friend or Family Member Not Included in Category Above)” category when the requested length of time the installation pass is valid exceeds 90 days (para 24f).
- Increase from Bravo to Charlie the FPCON restriction for the “Official Guest” category (para 25j).
- Replace installation-pass application memorandums with AE Form 190-16A (fig 2).
- Add nonappropriated fund (NAF) grades and additional noncommissioned officer (NCO) ranks to the sponsoring-official authorization paragraph (para 28b(2)(c)).
- Add guidance for handling installation-pass requests when the category requires background checks but the applicant is not eligible to have the check conducted (para 28b(5)(d)).
- State that copies of all background-check results are required when applying for an installation pass (para 28d(2)).
- Add guidance for IACS registrars to check to see if access less than USAREUR-wide is applicable when the application requests USAREUR-wide access (para 35a(4)).
- Add the “Print Summary Page” from the IACS Registration module as part of the installation-pass application packet (para 35a(6)).
- Update the Privacy Act Statement (fig 6).
- Add a paragraph that states individuals will not use sign-in procedures to avoid the installation-pass process or access-roster requirements (para 38b(3)).

Applicability. This regulation applies to personnel requiring access to U.S. Forces-controlled installations. The 22d ASG and 80th ASG may develop policy and procedures that meet or exceed the standards of this regulation to meet their unique needs.

Supplementation. Commanders will not supplement this regulation without Provost Marshal (PM), USAREUR (AEAPM-O-SO), approval.

Forms. This regulation prescribes AE Form 190-16A. 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. File numbers and descriptions are available on the Army Records Information Management System website at <https://www.arims.army.mil>.

NOTE: In connection with the collection, processing, and submission of data of local national employees in Germany, organizations of the U.S. Forces must adhere to the provisions of the U.S. Privacy Act; other than that, the U.S. Privacy Act, as U.S. national law, does not apply to local national employees in Germany.

Suggested Improvements. The proponent of this regulation is the USAREUR PM (AEAPM-O-SO, DSN 381-7224). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

Distribution. A (AEPUBS).

CONTENTS

SECTION I GENERAL

1. Purpose
2. References
3. Explanation of Abbreviations and Terms
4. General
5. Responsibilities
6. Policy
7. Exceptions to Policy

SECTION II INSTALLATION ACCESS

8. Access Methods
9. DOD ID-Card-Holder Access to Installations
10. Installation Passes

SECTION III INSTALLATION ACCESS CONTROL SYSTEM

11. IACS Registration
12. DOD ID-Card Holder
13. Local National Employee
14. Contractor (Based in United States)
15. Contractor (Living in Host Nation)
16. Personal-Service Employee
17. Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract)
18. Vendor or Commercial Solicitor
19. NATO Member
20. Host-Nation Military Member
21. Foreign Student (Marshall Center)
22. Member of Private Organization
23. Visitor (Immediate Family Member Living in Europe)
24. Visitor (Friend or Family Member Not Included in Category Above)
25. Official Guest
26. Department of State and American Embassy Personnel
27. Other

**SECTION IV
INSTALLATION PASS**

- 28. Application Process
- 29. Application Procedures for Applicant With Temporary Installation Pass
- 30. Application Procedures for Renewal Pass
- 31. Application Procedures for Lost or Stolen Pass
- 32. Application Procedures for Extension of Temporary Pass
- 33. Unserviceable Pass

**SECTION V
INSTALLATION ACCESS CONTROL OFFICE**

- 34. General
- 35. Registration Procedures for Installation-Pass Applicant
- 36. Registration Procedures for DOD ID-Card Holder
- 37. Processing Access Rosters

**SECTION VI
ACCESS PROCEDURES**

- 38. Sign-In Procedures
- 39. Access Rosters
- 40. Emergency-Vehicle and Protective-Services-Vehicle Access
- 41. ACP Guards

Appendix

- A. References

Figures

- 1. Sample Temporary USAREUR/USAFE Installation Pass and USAREUR/USAFE Installation Pass
- 2. Sample AE Form 190-16A
- 3. Height and Weight Conversion Chart
- 4. Format for Designation of Sponsoring Official's Memorandum
- 5. Sample Installation-Pass-Holder Acknowledgment of Responsibilities
- 6. Privacy Act Statement

Glossary

**SECTION I
GENERAL**

1. PURPOSE

This regulation—

- a. Prescribes policy, responsibilities, and procedures for granting access to U.S. Forces installations in the USAREUR area of responsibility (AOR).
- b. Provides registration procedures for the Installation Access Control System (IACS).
- c. Provides procedures for preparing and issuing installation passes.
- d. Must be used with the following regulations:
 - (1) AR 600-8-14.
 - (2) AE Regulation 190-13.

(3) USAREUR Regulation 525-13.

(4) USAREUR Regulation 600-700.

(5) USAREUR 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 Technical Manual (TM) 5-853-2 or provided by the installation antiterrorism officer, the physical security officer, or the United States Army Installation Management Agency, Europe Region Office (IMA-Europe).

b. USAREUR Regulation 525-13 prescribes policy and procedures for physically searching individuals and vehicles.

c. Installation-access control in the USAREUR AOR depends on the successful use of the IACS. The IACS—

(1) Minimizes access to installations by persons using forged, invalid, or unauthorized access documents.

(2) Includes a database on individual-access privileges.

(3) Allows for centralized control of access privileges (for example, commanders may withdraw a terminated employee's access authorization).

(4) Produces installation passes.

(5) Enables ACP guards (referred to as "guards" in this regulation) to scan barcoded DOD identification (ID) cards and installation passes to verify access authorization and privileges.

(6) Provides an automated historical record of personnel who have accessed U.S. Forces installations.

d. Sponsoring organizations and officials are critical to the success of the Installation Access Control Program.

e. Individual access privileges are risk-based and depend on an individual's category (paras 12 through 27).

5. RESPONSIBILITIES

a. The USAREUR G2 will—

(1) Manage the Foreign National Screening Program (USAREUR Reg 604-1).

(2) Provide an automated system to support the foreign national screening (FNS) process.

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

c. 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 U.S. Forces-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 the 1st Personnel Command (1st PERSCOM) and area support groups (ASGs) to ensure that the IACS database accurately shows all barred individuals.

d. The Commander, 1st PERSCOM, 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 bars to installations and develop procedures for providing timely updates to bar rosters so that the IACS remains current and accurate.

e. ASG commanders will—

(1) Develop policy to ensure access to base support battalions (BSBs) is controlled according to this regulation. ASG and BSB installation-access-control policy must not circumvent this regulation. For example, ASG commanders will not develop policy that honors only installation passes issued by their ASG or one of their subordinate BSBs. 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. This does not include situations in which the guard has reason to question the authenticity of the access document.

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

(3) Establish procedures for coordinating with sponsoring organizations to determine access authorization for an installation-pass applicant when the results of a background check include derogatory information. This may be delegated to the BSB when access is limited to a single BSB.

(4) When an applicant is requesting access to more than one ASG, send the results of the background check with derogatory information to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

(5) Develop procedures to notify the USAREUR PM of bars originating from an ASG that are not U.S. Forces-wide bars.

(6) Fulfill sponsoring-organization responsibilities where this regulation designates the ASG 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.

f. In addition to the responsibilities in subparagraph e above, the 22d ASG and 80th ASG commanders 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, residence and work permits). The adapted policy and procedures must—

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

(2) Be coordinated with and approved by the USAREUR PM and the Judge Advocate (JA), USAREUR.

g. BSB commanders will—

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

(a) Procedures for DOD ID-card holders to register in and withdraw from the IACS during in- and outprocessing at either their servicing IACO or central processing facility (CPF).

(b) Procedures for retrieving installation passes from individuals who no longer require installation access.

(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-card holders.

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.

4. Procedures for responding to vehicle drivers who disregard guard instructions (for example, failure to stop for access verification).

5. A picture sample of the USAREUR/USAFE Installation Pass, the Temporary USAREUR/USAFE Installation Pass, and each type of DOD ID card.

6. Contact rosters for key personnel.

7. Map of the installation.

8. Telephone numbers for key organizations on the installation being guarded.

9. Random antiterrorism measures and force protection condition (FPCON) guidance.

10. Use-of-force guidance.

(e) Provide a copy of the ACP policy to the local German works council.

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

(3) 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.

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

(5) Ensure all IACS hardware transferred to the BSB is dedicated to support the IACS.

(6) Fulfill sponsoring-organization responsibilities where this regulation designates the BSB as the sponsoring organization.

h. BSB and area support team (AST) provost marshal offices (PMOs) 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 military police (MP) background checks required for installation passes (para 28b(5)). Copies of MP 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 ASG. ASG policy for processing background checks that result in derogatory information must be followed.

i. 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 residence and work permits 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, quits, is terminated).

(3) Develop procedures to ensure requiring activities (k 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 in the USAREUR AOR:

(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.

j. Section V explains IACO responsibilities.

k. 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).

(3) Background checks on individuals seeking an installation pass are completed. When any derogatory information is discovered, the sponsoring organization must coordinate with the host ASG (or USAREUR PM if USAREUR-wide access is requested) to determine if the derogatory information should warrant 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 in the USAREUR AOR:

(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.

NOTE: If contractor access is not required, instead of providing the information in (a) and (b) above, sponsoring organizations may include the statement "This contract will not result in a contractor requiring access to a U.S. Forces installation."

(6) Contracting officers outside the purview of United States Army Contracting Command, Europe, 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 are 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 that designates persons authorized to perform sponsoring-official duties on behalf of the sponsoring organization (fig 4) is sent to the servicing IACO.

(11) Procedures in paragraph 28c are followed when the sponsoring official cannot escort the applicant to the servicing IACO.

l. 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-card holder has a manually produced DOD ID card, that individual must obtain a machine-produced, barcoded DOD ID card according to the 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 the USAREUR AOR must request an installation pass. The installation pass will 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 the immediate surrender of 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 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 his or her POV as part of the installation-pass-application process if planning to use the POV to enter U.S. Forces-controlled installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

m. Paragraph 41 prescribes access-control-guard responsibilities.

6. POLICY

a. 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 reason to circumvent or modify the procedures established by this regulation. These procedures will help—

(1) Support FPCON measures related to installation-access control.

(2) Identify barred individuals at U.S. Forces-installation ACPs.

(3) Prevent wrongful possession and pilferage of Government property and unlawfully bringing weapons, explosives, and other contraband onto U.S. Forces installations.

b. DFMD policy is as follows:

(1) Inprocessing. Personnel who possess an authorized DOD ID card and installation-pass applicants will provide DFMD during the IACS registration process.

(2) Identity Verification. Security or appropriate command personnel may require an individual to provide his or her DFMD for identity verification. This verification may routinely occur at ACPs to U.S. Forces installations. It may also occur at locations beyond the ACP. Refusal to provide DFMD may be the basis for immediate surrender of the individual's installation pass or DOD ID card and grounds for further administrative or punitive action by the command. If the request for the DFMD extends beyond identifying an individual, "probable cause" or other legal basis must be present before any apprehension or search. Coordination must be made with—

(a) The servicing staff judge advocate office (when practical) if the request for the DFMD leads to an apprehension or search.

(b) Host-nation police if the apprehension or search involves a local-nation citizen. If it involves a local-national employee, the appropriate works council will also be consulted during official duty hours. If a local-national employee is being apprehended or searched outside official duty hours, the appropriate works council will be informed immediately on the next workday.

c. The installation-access policy is based on verifying the access authorization of every individual entering a controlled U.S. Forces installation, not vehicles or other means of transportation used to gain access. All individuals in vehicles or other modes of transportation will have their access-authorization verified according to the policy and procedures in this regulation.

7. EXCEPTIONS TO POLICY

a. Persons requesting an exception to any policy in this regulation must send their request through appropriate command channels to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931, or by e-mail to iacs@manupo.pmo.army.mil.

b. All exceptions to policy that were approved before this regulation was published are no longer valid. Exceptions to policy approved after this regulation takes effect may be authorized and approved by the USAREUR PM for up to 1 year. Only the USAREUR PM may provide an exception to policy for a longer period and will do so only in writing.

c. Exceptions to policy that are imbedded in the IACS software application may be administered locally and do not require USAREUR PM approval.

d. Exceptions to policy outlined in paragraph 8b are not subject to this paragraph.

SECTION II INSTALLATION ACCESS

8. ACCESS METHODS

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

(1) Have a valid DOD ID card and be registered in the IACS (unless the exception to registration requirements in paragraph 40e applies).

(2) Have a USAREUR/USAFE Installation Pass or a Temporary USAREUR/USAFE Installation Pass. A valid installation pass with TDY orders will authorize access when an individual must temporarily exceed his or her access level for operational reasons. For example, if an installation-pass holder has a 6th ASG-wide installation pass but must attend training in the 26th ASG AOR, his or her installation pass with TDY orders stating the training location and dates will be used to allow access. Because not all of these situations involve the issuance of TDY orders, other documents that state the purpose of travel and the location and dates are acceptable.

(3) Be signed in by an individual with sign-in privileges.

(4) Be on an approved access roster and present one of the documents listed in paragraph 28d(1).

b. The methods in subparagraph a above should be used with the policy and procedures in this regulation whenever possible. There may be situations, however, when commanders must supplement those methods 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 explained in BSB policy and approved by the ASG commander. This subparagraph does not negate the policy in paragraph 7.

c. Paragraph 40 explains access policy for emergency and protective-services vehicles.

d. Memorandums, travel orders, AE Form 600-700A, a U.S. passport, NATO Sending State (Belgian, British, Canadian, Dutch, and French) ID cards, and DD Form 1172 are not access-authorization documents. Guards will not grant access based only on these documents. Individuals with these types of documents must be signed in by someone with sign-in privileges. All persons who used to obtain recurring, unescorted access using one of these or other types of documents must obtain an installation pass using the appropriate person category (paras 12 through 27).

e. 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, USAREUR/USAFE Installation Passes, or Temporary USAREUR/USAFE Installation Passes.

f. 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 immediately will 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.

9. DOD ID-CARD-HOLDER ACCESS TO INSTALLATIONS

a. A DOD ID card does not automatically authorize the cardholder access to U.S. Forces installations in the USAREUR AOR. The DOD ID card must have a readable barcode and the DOD ID-card holder must be registered in the IACS, unless the exception to the registration requirement in paragraph 41e applies. Personnel with a manually produced DOD ID card must obtain a machine-produced DOD ID card with a barcode according to the procedures established by appropriate military regulations and personnel systems.

b. The following machine-produced DOD ID cards (AR 600-8-14) are considered valid access documents:

(1) DD Form 2(ACT). This green card is issued to active duty military personnel. This card is being replaced by the Common Access Card (CAC) ((11) below).

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

(3) DD Form 2(RET). This red or green card is issued to Reserve or National Guard personnel.

(4) DD Form 2(RES RET). This red card is issued to Reserve and National Guard retirees.

(5) DD Form 489. This card is issued to civilian noncombatants authorized to accompany the U.S. Armed Forces into combat regions and who may become prisoners of war.

(6) DD Form 1173. This tan card is issued to eligible military and DOD civilian-employee family members.

(7) DD Form 1173-1. This red card is issued to eligible Reserve and National Guard military and DOD civilian-employee family members.

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

(9) DD Form 2764. This tan card is issued to emergency-essential civilians and civilian-contract employees.

(10) DD Form 2765. This tan card is issued to general-schedule employees and DOD contractors who receive logistical support.

(11) CAC.

NOTE: Most CACs are made from white plastic card stock with no identifying color markings. CACs with a green stripe are sometimes issued to DOD contractors, who will be processed as DOD ID-card holders for the purpose of IACS registration. CACs with a red vertical stripe on the right side of the card will not be recognized as an authorized access document. The red-striped CAC is issued to local national (LN) employees. LN employees must obtain an installation pass for access according to paragraph 13.

10. INSTALLATION PASSES

a. The two types of installation passes are the USAREUR/USAFE Installation Pass and the Temporary USAREUR/USAFE Installation Pass, which are referred to as “Installation Pass” and “Temporary Installation Pass,” respectively.

b. Temporary Installation Passes have a red background in the title block to distinguish them from the Installation Pass, which has a green background. Figure 1 shows samples of both passes. Although these installation passes are similar in appearance, the restrictions associated with each pass are different.

c. IACOs will not alter the appearance of installation passes with ASG- or BSB-unique features (for example, custom stamps, stickers, holograms).

d. The differences between the Temporary Installation Pass and Installation Pass include the following:

(1) A Temporary Installation Pass is valid for up to 90 days.

(2) If an Installation Pass is desired, a Temporary Installation Pass may be issued pending completion of a required background check. This balances security concerns with operational requirements. The use of successive Temporary Installation Passes is unauthorized, unless the exception in paragraph 32 applies.

e. Paragraph 11 provides requirements for registering installation-pass applicants into the IACS. The application procedures in paragraphs 12 through 27 must be completed before IACS registration may begin.

SECTION III INSTALLATION ACCESS CONTROL SYSTEM

11. IACS REGISTRATION

a. All DOD ID-card holders assigned in the USAREUR AOR and installation-pass applicants must be registered in the IACS. DOD ID-card holders who are on TDY orders to or visiting the USAREUR AOR may also be registered, depending on the length of their stay. For example, an individual with TDY orders to Germany for 2 days may not need to be registered, but an individual who will be on TDY in Germany for 1 month should be registered.

b. Access by a nonregistered DOD ID-card holder will be recorded in the IACS. This procedure may cause nonregistered DOD ID-card holders a minor delay each time they enter an installation. The IACS also will track excessive numbers of times nonregistered DOD ID-card holders enter an installation. This will help identify possible unauthorized DOD ID-card holders (para 40e).

c. Section IV provides application procedures for installation passes.

d. An individual may qualify for one of the following categories:

(1) DOD ID-Card Holder.

(2) Local National Employee.



Figure 1. Sample Temporary USAREUR/USAFE Installation Pass and USAREUR/USAFE Installation Pass

- (3) Contractor (Based in United States).
- (4) Contractor (Living in Host Nation).
- (5) Personal-Service Employee.
- (6) Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract).
- (7) Vendor or Commercial Solicitor.
- (8) NATO Member.
- (9) Host-Nation Military Member.
- (10) Foreign Student (Marshall Center).
- (11) Member of Private Organization.
- (12) Visitor (Immediate Family Member Living in Europe).
- (13) Visitor (Friend or Family Member Not Included in Category Above).
- (14) Official Guest.
- (15) Department of State and American Embassy Personnel.

(16) Other.

e. A dual-category individual (for example, a military retiree who is also a contractor) will be registered in the category that provides the greatest access privileges. The Official Guest (d(14) above) and Other (d(16) above) categories will never be used as a dual-category qualifier.

f. The categories in subparagraph d above are risk-based. Paragraphs 12 through 27 provide specific requirements for registration and access restrictions for each category.

12. DOD ID-CARD HOLDER

a. Definition. An individual authorized to possess a DOD ID card, including children under the age of 18. The status of a DOD ID-card holder will supersede other person categories (para 11d(2) through (16)). For example, an LN employee married to a servicemember and entitled to DD Form 1173 will be treated as a DOD ID-card holder for the purpose of this regulation and will not be issued an installation pass or be required to be sponsored.

b. Type of Pass Authorized. Individuals possessing an authorized DOD ID card will obtain their ID card through procedures established by appropriate military regulations and personnel systems. These individuals must register at their servicing IACO or CPF during community inprocessing to be registered in the IACS but will not be issued an installation pass. If the DOD ID-card holder has a manually produced DOD ID card, that person must obtain a machine-produced (barcoded) DOD ID card. Individuals who have multiple DOD ID cards (for example, a military retiree who is now a DA civilian employee) must choose which DOD ID card they want to use for IACS registration and use this card to access the installation.

c. Length of Time Registration Is Valid. For personnel with an established date eligible for return from overseas (DEROS), registration is valid 15 days past their DEROS or until the expiration date of their DOD ID card, whichever is earlier. In no case will the registration period exceed 5 years. For individuals that are in the USAREUR AOR temporarily (for example, on TDY), the registration period will be based on their established departure date.

NOTE: Because the IACS will always establish an expiration date of registration, it is critical for anyone granted an extension (for example, a soldier with an approved foreign-service tour extension) to visit their servicing IACO or CPF to update the expiration date in the IACS.

d. Sponsor Requirements. Unlike people in other categories, DOD ID-card holders may sponsor themselves and do not need to submit an installation-pass application (AE Form 190-16A). DOD ID-card holders will provide the IACO or CPF the documentation that supports the requirement to be registered in the IACS. This documentation will also be used to determine the expiration date for many individuals. Examples of acceptable documentation include, but are not limited to, permanent change of station (PCS) and TDY orders, DA Form 31, SF 50-B, and DA Form 3434. The purpose of this documentation is to prevent individuals who illegally possess a DOD ID card from being registered in the IACS. Minors will be registered in the presence of a parent or legal guardian.

e. Background Checks. Background checks are not required for DOD ID-card holders.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a DOD ID-Card Holder May Enter. No restrictions apply unless imposed by an authorized commander.

h. Restrictions on Days and Times Access Is Authorized. No restrictions apply unless imposed by an authorized commander.

i. Restrictions on Sign-In Privileges. The DOD ID-card holder must be at least 18 years old. This privilege is limited to signing in four persons and their vehicles. No other restrictions apply unless imposed by an authorized commander.

NOTE: Commanders may restrict or withdraw individual access or privileges depending on the circumstances after consulting with the servicing staff judge advocate and IACO.

j. FPCON Restrictions. No restrictions apply.

13. LOCAL NATIONAL EMPLOYEE

a. Definition. An individual who is employed by DOD in the USAREUR AOR and is not entitled to one of the DOD ID cards listed in paragraph 9b. This category is primarily for host-nation employees in the USAREUR AOR.

NOTE: LN employees may be issued a CAC as DOD transitions to the requirement for all DOD-computer users to use a CAC to log onto Government computers. CACs issued to LN employees will have a red vertical stripe down the right side of the CAC. These CACs will not be used as installation-access documents.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized after all required background checks have been completed and an FNS has been initiated. The Temporary Installation Pass will be used only until an Installation Pass is authorized.

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed.

c. Length of Time Pass Is Valid. A Temporary Installation Pass is valid for up to 90 days. An Installation Pass is 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.

d. Sponsor Requirements. The organization that the LN employee will work for 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.

(2) MP Check. This check is required before a Temporary Installation Pass may be issued.

(3) Defense Clearance and Investigation Index (DCII). If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before a Temporary Installation Pass may be issued.

(4) FNS. This screening must be initiated before a Temporary Installation Pass is issued; it must be completed before an Installation Pass is issued. Employees hired before 3 October 1985 are exempt from this requirement (USAREUR Reg 604-1).

f. Residence and Work Permits. These permits may be required if the applicant is not a European Union (EU) resident.

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

h. Restrictions on Days and Times Access Is Authorized. No restrictions apply unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Temporary Pass holders are not authorized sign-in privileges. Installation Pass holders 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 are not authorized during FPCON Delta.

j. FPCON Restrictions. No FPCON restrictions apply.

14. CONTRACTOR (BASED IN UNITED STATES)

a. Definition. A person who lives in the United States and is contracted to work for DOD in the USAREUR AOR, but is not a DOD ID-card holder. Although this person category is authorized an Installation Pass, the pass is specially designed for contractors from the United States, but working in the USAREUR AOR temporarily.

NOTE: A person must be contracted to work for DOD to obtain an installation pass. Contractors who are only attempting to establish a contract with DOD will obtain access to U.S. Forces installations in the USAREUR AOR by an individual with sign-in privileges or through access-roster procedures.

b. Type of Pass Authorized.

(1) Temporary Installation Pass.

(2) Installation Pass. This pass may be authorized only if the person will be in the USAREUR AOR longer than 90 consecutive days.

c. Length of Time Pass Is Valid. The Temporary Installation Pass is valid for the length of the visit or up to 90 days, whichever is less. The Installation Pass is valid for the length of the visit (must be more than 90 consecutive 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 earlier.

d. Sponsor Requirements. The organization inviting the contractor to or escorting the contractor in the USAREUR AOR will perform the sponsor responsibilities in this regulation.

e. Background Checks. No background checks are required for persons in this category.

f. Residence and Work Permits. A residence permit may be required (para 28b(6)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be 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 unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. People in this category are not authorized to sign in guests.

j. FPCON Restrictions. No FPCON restrictions apply.

15. CONTRACTOR (LIVING IN HOST NATION)

a. Definition. A contractor who lives in the host nation, is contracted to work for DOD in the USAREUR AOR, and is not a DOD ID-card holder.

NOTE: A contractor must be contracted to work for DOD to obtain an installation pass. Contractors who are only attempting 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. This pass may be authorized only after all required background checks are completed and an FNS has been initiated.

(2) Installation Pass. This pass may be authorized only after all required background checks (including an FNS) have been completed.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for the length of the contract or up to 90 days, whichever is less. The 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 earlier.

d. Sponsor Requirements.

(1) Unlike people in other categories, identifying the sponsoring organization may be more difficult for this type of contractor. In general, the organization hiring the contractor will perform the sponsor responsibilities in this regulation. Hiring organizations will not request access for the contractor that extends beyond their needs. For example, if an organization is going to have furniture delivered to two installations in a BSB, the hiring organization will not sponsor the contractor for an installation pass that allows access to more than the BSB.

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

(a) When access to more than three ASGs is requested, the request will be considered the same as “USAREUR-wide.” Specifically, requests that include access to more than three ASGs may be approved only by the following organizations, which will perform sponsoring-organization responsibilities:

1. HQ USAREUR/7A staff office.
2. IMA-Europe.
3. Department of Defense Dependents Schools-Europe.
4. United States Army Corps of Engineers, Europe District.
5. 5th Signal Command.
6. 66th Military Intelligence Group.
7. 202d Military Police Group.
8. United States Army Europe Regional Medical Command.
9. United States Army Europe Regional Dental Command.
10. United States Army Center for Health Promotion and Preventive Medicine - Europe.
11. United States Army Medical Materiel Center, Europe.
12. Army and Air Force Exchange Service, Europe (AAFES-Eur).
13. United States Army Materiel Command, Europe.
14. Defense Commissary Agency, European Region.
15. Seventh Army Training Command.

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

(b) When access is required to two or three ASGs, the rank and grade requirements of paragraph 28b(2)(c)4 apply; however, the sponsoring organization need not be one of the organizations in (a) above. The sponsoring organization will be the ASG where the contractor is headquartered or performs most of his or her business.

(c) Contractors whose service exceeds one BSB but is limited to one ASG may obtain an Installation Pass for that ASG. The sponsoring organization must be the ASG.

(d) In all other cases, sponsoring organizations are not authorized to sponsor an Installation-Pass applicant beyond the BSB.

(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 USAREUR AOR based on individual contracts with several organizations should obtain an installation pass for the ASG or BSB where they conduct most of their business and use sign-in procedures or site-specific access rosters for other locations. Paragraph 38 explains unique access-roster requirements for contractors.

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before a Temporary Installation Pass or Installation Pass may be issued.

(2) MP Check. This check is required before a Temporary Installation Pass or Installation Pass may be issued.

(3) DCII. If the applicant claims previous affiliation with the U.S. Armed Forces and has a social security number, this check must be completed before a Temporary Installation Pass or Installation Pass may be issued.

(4) FNS. This screening must be completed for non-U.S. citizens before an Installation Pass is issued. The FNS does not have to be completed before issuing a Temporary Installation Pass.

f. Residence and Work Permits. These permits may be required for non-German citizens, unless the non-German citizen has an exception to this requirement (para 28b(6)(d)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be 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 unless specified by the sponsor organization.

i. Restrictions on Sign-In Privileges. Sign-in privileges normally are not granted to contractors. As an exception, primary contractors (contractors who report directly to a DOD ID-card holder or full-time LN employee) may be granted sign-in privileges when the sponsoring official is at least a lieutenant colonel or civilian equivalent (GS-13 or C-8). The 22d ASG and 80th ASG may use the equivalent paygrade for their LN employees. Sign-in privileges are not authorized at FPCON Delta and will be limited to signing in four people and their vehicles. Only other contractors and vendors that support the contract may be signed in. Sign-in privileges are not authorized for Temporary Installation Pass holders.

j. FPCON Restrictions. The Temporary Installation Pass allows access during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization. There are no restrictions for the Installation Pass.

16. PERSONAL-SERVICE EMPLOYEE

a. Definition. An individual hired by someone (see “requester” in glossary) to perform a service (for example, as nanny, dog-sitter, house-cleaner).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized after all required background checks except the FNS have been completed (see e(4) below).

(2) Installation Pass. This pass may be authorized after all required background checks (including an FNS) have been completed.

c. Length of Time Pass Is Valid. The Temporary Installation Pass is valid for the length of service or up to 90 days, whichever is earlier. The Installation Pass is 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 earlier.

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

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before a Temporary Installation Pass or Installation Pass may be issued.

(2) MP Check. This check is required before a Temporary Installation Pass or Installation Pass may be issued.

(3) DCII. If the applicant claims previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before a Temporary Installation Pass or Installation Pass may be issued.

(4) FNS. This screening is required for non-U.S. citizens before an Installation Pass may be issued. The FNS does not have to be completed to issue a Temporary Installation Pass.

f. Residence and Work Permits. These permits may be required for non-German citizens, unless the non-German citizen has an exception to this requirement (para 28b(6)(d)).

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

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

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

j. FPCON Restrictions. The Temporary Installation Pass allows access during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization. There are no restrictions for the Installation Pass.

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

a. Definition. An individual who needs recurring access to U.S. Forces installations to make deliveries or perform a similar service that is related to his or her employment (for example, pizza delivery, taxi driver).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized after all background checks (e below) have been completed.

c. Length of Time Pass Is Valid. The Installation Pass will be valid for up to 2 years or expire on 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 BSB being serviced will be the sponsor for people in this category.

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before an Installation Pass may be issued.

(2) MP Check. This check must be completed before an Installation Pass may be issued.

(3) DCII. If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) FNS. An FNS is required for non-U.S. citizens to receive an Installation Pass.

f. Residence and Work Permits. These permits are required for non-German citizens. Paragraph 28b(6)(d) 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 BSB. The sponsoring BSB may impose further restrictions (for example, to only certain caserns). Access may be extended to the ASG only if the ASG is willing to accept sponsoring-organization responsibilities.

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

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

j. FPCON Restrictions. Installation Passes for delivery personnel are valid only at FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

18. VENDOR AND COMMERCIAL SOLICITOR

a. Definition. An individual who is authorized to sell merchandise or provide services on U.S. Forces installations.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed.

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 commercial solicitation or vendor permit that was issued by 1st PERSCOM, whichever is earlier.

d. Sponsor Requirements. The sponsoring organization will be the BSB when access requested does not exceed the BSB. The sponsoring organization will be the ASG when access requested exceeds one BSB but is limited to one ASG. When access is for more than one ASG, the applicant must be sponsored by AAFES-Eur, Defense Commissary Agency, European Region, 1st PERSCOM, or IMA-Europe. This sponsoring authority may not be delegated to subordinate organizations.

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before an Installation Pass may be issued.

(2) MP Check. This check is required before an Installation Pass may be issued.

(3) DCII. If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) FNS. An FNS must be completed for non-U.S. citizens to receive an Installation Pass.

f. Residence and Work Permits. These permits are required for non-German citizens, unless the non-German citizen is an exception to this requirement according to paragraph 28b(6)(d).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations a pass holder may enter 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 access days or times unless specified by the sponsor.

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

j. FPCON Restrictions. Installation passes are only valid during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

19. NATO MEMBER

a. Definition. NATO military personnel, civilian employees, and their family members who reside in Germany or who meet the requirements in USAREUR Regulation 600-700, chapters 20 through 22. This category is designed for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military stationed in Germany) and should not be confused with the Host-Nation Military Member category in paragraph 20.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass is authorized for NATO Member personnel described in subparagraph a above.

c. Length of Time Pass Is Valid. This pass will be valid for up to 5 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.

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

(2) Active-Duty Belgian, British, Canadian, Dutch, and French Military Stationed in Germany (also known as Sending States). The security office from the Sending State will sponsor people in this category. The Sending State will submit a memorandum designating sponsoring officials to the USAREUR PM by e-mail (iacs@manupo.pmo.army.mil). The PM will post this memorandum to the restricted portion of the IACS website, where it will be available to all USAREUR IACOs. Individuals in this category may obtain an Installation Pass at any IACO. Because these individuals are stationed throughout Germany, the 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 28c.

(3) French and British Consular and Diplomatic Personnel Stationed in Germany. The U.S. Mission, Germany (U.S. Department of State), will sponsor people 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 will be available to all USAREUR 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 28c.

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

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. There are no restrictions. NATO Members are automatically granted access to U.S. Forces installations and facilities. No justification for access will be required.

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

i. Restrictions on Sign-In Privileges. People in this category will be limited to signing in four people and their vehicles.

j. FPCON Restrictions. No FPCON restrictions apply.

20. HOST-NATION MILITARY MEMBER

a. Definition. A member of the host-nation military who works or resides on a U.S. Forces-controlled installation in the nation they serve (for example, German soldiers in Germany, Italian soldiers in Italy). This category should not be confused with the NATO Member category (para 19), which is designed specifically for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military stationed in Germany).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. Persons in this category will receive an Installation Pass.

c. Length of Time Pass Is Valid. The Installation Pass for a Host-Nation Military Member will be valid for up to 5 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 will be the sponsoring organization and perform the sponsor responsibilities. If no such organization exists, the BSB will perform the sponsor responsibilities.

e. Background Checks. No background checks are required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on the Number of Installations a Pass Holder May Enter. The number of installations a pass holder may enter will be 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 access times unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Installation-Pass holders 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 FPCON restrictions apply.

21. FOREIGN STUDENT (MARSHALL CENTER)

a. Definition. Foreign military students assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany.

b. Types of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass is authorized for people in this category.

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 earlier.

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

e. Background Checks. No background check is required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installation a Pass Holder May Enter. Access will not exceed installations in the Garmisch AST.

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

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

j. FPCON Restrictions. No FPCON restrictions apply.

22. MEMBER OF PRIVATE ORGANIZATION

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

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized after all background checks (including FNS) have been completed.

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 BSB where the private-organization function takes place will perform sponsor responsibilities.

e. Background Checks.

(1) Police Good Conduct Certificate (*Polizeiliches Führungszeugnis*). This certificate is required before an Installation Pass may be issued.

(2) MP Check. This check must be completed before an Installation Pass is issued.

(3) DCII. If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) FNS. An FNS is required for non-U.S. citizens.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

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

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days and times of access unless imposed by the sponsoring BSB.

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

j. FPCON Restrictions. Installation Passes are valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

23. VISITOR (IMMEDIATE FAMILY MEMBER LIVING IN EUROPE)

a. Definition. An individual who is an immediate family member of the requester (glossary) and lives in Europe. In this regulation, “immediate family members” include the requester’s son, daughter, mother, father, brother, sister, mother-in-law, father-in-law, brother-in-law, sister-in-law, grandparents, and grandparents-in-law.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized only when the requester resides on a controlled-access installation.

c. Length of Time Pass Is Valid. The Installation Pass will be valid until the requester’s DEROS 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 BSB where the requester resides will be the sponsor for people in this category and will perform sponsor responsibilities.

e. Background Checks. No background checks are required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring BSB. The sponsoring BSB may impose further restrictions.

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

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

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

24. VISITOR (FRIEND OR FAMILY MEMBER NOT INCLUDED IN CATEGORY ABOVE)

a. Definition. A visiting family member or friend of the requester (glossary) who is not included in the category in paragraph 23. Applicants must prove that they are staying with the requester and have an established departure date. This category will not be used to allow local friends or local people who are not immediate family members unescorted access to U.S. Forces installations.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. People in this category may be issued a Temporary Installation Pass.

(2) Installation Pass. People in this category may be issued an Installation Pass only if they are family members.

c. Length of Time Pass Is Valid. The Temporary Pass will be valid for the length of the visit or up to 90 days, whichever is less. An 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 earlier.

d. Sponsor Requirements. The BSB where the requester resides will be the sponsor for people in this category and will perform the sponsor responsibilities.

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

f. Residence and Work Permits. A residence permit will be required if an Installation Pass is going to be issued for more than 90 days.

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

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

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

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

25. OFFICIAL GUEST

a. Definition. A broad category designed for individuals requiring recurring access for official business or access based on an official relationship (for example, official visits from other Federal agencies such as the Federal Aviation Administration, or visits by local city officials such as the mayor, fire chief, or an employee of the German Construction Office (*Bauamt*)). 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. People in this category may be issued Temporary Installation Passes.

(2) Installation Pass. People in this category may be issue an Installation Pass.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for up to 90 days. An 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 ASG or BSB will be the sponsor for people in this category and will perform the sponsor responsibilities.

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

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

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

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

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

j. FPCON Restrictions. Installation passes will be valid only through FPCON Charlie; however, a one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

26. DEPARTMENT OF STATE AND AMERICAN EMBASSY PERSONNEL

a. Definition. An individual assigned to or on duty with the United States Department of State, an American Embassy in the USEUCOM AOR, or in U.S. diplomatic or consular posts according to USAREUR Regulation 600-700, chapter 28.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. People in this category may be issued an Installation Pass.

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) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The United States Mission, Germany, will be the sponsor for people in this category and will perform the sponsor responsibilities. The United States Mission, Germany, will submit a memorandum designating sponsoring official to the USAREUR PM by e-mail (iacs@manupo.pmo.army.mil). The PM will post this memorandum to the restricted portion of the IACS website, where it will be available to all USAREUR 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 the Installation Pass according to paragraph 28b.

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

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. There are no restrictions on the number of installations. Department of State and American Embassy personnel automatically receive access to U.S. Forces installations. No justification is required.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on when people in this category may access installations.

i. Restrictions on Sign-In Privileges. People in this category will be limited to signing in four people and their vehicles.

j. FPCON Restrictions. No FPCON restrictions apply.

27. OTHER

a. Definition. An individual who requires recurring and unescorted access, but who does not meet the definition of another category in paragraphs 12 through 26. Sponsoring organizations will not use this category if the applicant meets the definition of another, more restrictive category. An example for this category would be people who transport U.S. Forces employees to and from work on a daily basis.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. People in this category may be issued a Temporary Installation Pass.

(2) Installation Pass. People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for up to 90 days. An 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 BSB where access is required will be the sponsor for these people.

e. Background Checks. The sponsoring BSB will determine whether or not a background check is required.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

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

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

i. Restrictions on Sign-In Privileges. People in this category will not be authorized sign-in privileges.

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

SECTION IV INSTALLATION PASS

28. APPLICATION PROCESS

a. Sponsoring officials will help authorized individuals apply for an installation pass at the servicing IACO by preparing AE Form 190-16A (fig 2). AE Form 190-16A must be completed for the following reasons:

(1) To receive an initial installation pass (first-time pass).

(2) To obtain an Installation Pass after the applicant has received a Temporary Installation Pass (para 29).

APPLICATION FOR USAREUR/USAFE INSTALLATION PASS (AE Reg 190-16)						
DATA REQUIRED BY THE PRIVACY ACT OF 1974						
<p>Authority: Article 53, Supplementary Agreement to NATO SOFA; 10 USC 3012. Principal purpose(s): For identification of U.S. and non-U.S. nationals employed by U.S. Government agencies, contractors, and vendors of non-military agencies of countries in which U.S. personnel have been accommodated when these personnel require recurring access to the accommodations under U.S. control and do not possess other valid entry authorization documents. Routine use(s): To identify personnel authorized routine or recurring access to installations under U.S. control. Mandatory or voluntary disclosure and effect on individual not providing information: Voluntary. However, failure to provide any item of information will result in denial of entry onto the U.S.-controlled installations for which the AE Form 190-16A has been validated.</p>						
Please refer to the instructions on page 3 to ensure that the form is correctly filled in.						
1. To 293d BSB IACO Mannheim	2. From 5th Signal Command, Mannheim		3. Date (mm/dd/yyyy) 10/01/2003			
4. Applicant name (Last, first, MI) SCHMIDT, HANS L.	5. Sponsor address 5th Sig Cnd (NETC-SOP) CMR 420 APO AE 09056		6. Address (Company/Organization/Unit) 5th Sig Cnd (NETC-SOP) CMR 420 APO AE 09056			
7. Person category Local National Employee	8. Country of citizenship Germany		9. SSN/Personal ID number 4046750983			
10. Supporting document expiration date (Passport/ID card) (mm/dd/yyyy) 01/15/2005	11. Residence permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		12. Work permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No			
13. Type pass requested <input checked="" type="checkbox"/> Installation pass <input type="checkbox"/> Temporary installation pass	14. Date of birth (mm/dd/yyyy) 11/17/1964	15. Height (Inches) 71	16. Weight (Pounds) 170	17. Eye (Color) BLUE	18. Hair (Color) BROWN	
19. Installations for which access is required USAREUR-wide (Germany only)						
20. Limitations/time/day access is required 24/7		21. FPCON restriction DELTA		22. Pass expiration date (mm/dd/yyyy) 1/15/2005 IACO REGISTRAR MUST VALIDATE		23. Sign-in privileges <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
24. Privately owned vehicle (POV) registration information (additional vehicles may be added on a separate sheet of paper)						
a. License number MA-T123	b. Country Germany	c. Make Ford	d. Model Ka	e. Year 2003	f. Body type 2-door	g. Color White
25. Company name and telephone number						
26. Verification by sponsoring official authority						
<p>I have interviewed the applicant and reviewed the results of all background checks required by AE Reg 190-16. I verify that there is no derogatory information that would preclude the issuing of an installation pass. If approved, Mr./Mrs./Ms. <u>Schmidt</u>'s supervisor or a representative of my staff will counsel Mr./Mrs./Ms. <u>Schmidt</u> on the purpose and official uses of the installation pass. I have reviewed AE Reg 190-16 and believe this packet is administratively correct and fully and accurately portrays the basis for Mr./Mrs./Ms. <u>Schmidt</u>'s access requirements. However, if there is a problem or you need further information, please contact me.</p>						
a. Organization and telephone number 5th Sig Cnd 381-9303			b. Name and title COL BILL B BROWN G3			
c. Signature <i>Bill B Brown</i>			d. Date (mm/dd/yyyy) 10/1/2003			

AE FORM 190-16A, OCT 03

Page 1 of 3 pages

Figure 2. Sample AE Form 190-16A

27. Installations for which access is required (Provide justification)	
Mr. Schmidt's job involves conducting network infrastructure surveys in support of all the signal battalions in Germany. This requires him to travel to all the ASGs in Germany, hence USAREUR-wide access (Germany only) is required.	
28. Sign-in privileges (Provide justification)	
While conducting network infrastructure surveys, Mr. Schmidt must coordinate with and involve host nation telecommunications experts to ensure that DOD does not violate host-nation laws and statutes. This requirement necessitates that Mr. Schmidt is able to sign on these people to accomplish his job.	
Required attachments (Check applicable boxes)	
Requirements may be different depending on the person category selected. All installation-pass applications must include supporting documents. Some installation-pass applications may include a copy of:	
<input type="checkbox"/> Residence permit	<input type="checkbox"/> Defense Clearance Investigation Index (DCII)
<input type="checkbox"/> Work permit	<input checked="" type="checkbox"/> Proof of AE Form 604-1A, Foreign National Screening (FNS), initiation/completion
<input checked="" type="checkbox"/> Police Good Conduct Certificate (PGCC) (<i>Polizeiliches Führungszeugnis</i>)	<input checked="" type="checkbox"/> Military police (MP) check results

Figure 2. Sample AE Form 190-16A (Continued)

Instructions for completing AE Form 190-16A

<p>Item 1. To Enter the name of the servicing installation access control office.</p> <p>Item 2. From Enter the name of the sponsoring official's organization.</p> <p>Item 5. Sponsor address Enter the mailing address of the sponsoring organization. For the person categories Personal-Service Employee, Visitor (immediate family member living in Europe), and Visitor (friend or family member not included in the "immediate family member living in Europe)" category, also include the requester's mailing address.</p> <p>Item 6. Address Enter the address of the unit of assignment. This address will depend on the applicant's person category. For example, for local national employees, enter the hiring organization's address. For Contractors and Delivery Personnel, enter the address of their company. Visitors should list their home mailing address.</p> <p>Item 7. Person category</p> <table border="0"> <tr> <td> <ul style="list-style-type: none"> • DOD ID-card holder • Local national employee • Contractor (based in United States) • Contractor (living in host nation) • Personal-service employee • Delivery personnel (recurring deliveries or similar service not associated with a Government contract) • Vendor or commercial solicitor • NATO member • Host-nation military member </td> <td> <ul style="list-style-type: none"> • Foreign student (Marshall Center) • Member of private organization • Visitor (immediate family member living in Europe) • Visitor (friend or family member not included in category above) • Official guest • Department of State and American Embassy personnel • Other </td> </tr> </table> <p>Item 9. SSN/Personal ID number Enter the personal ID number or the passport number from the supporting document used. Applicant must have one of the following supporting documents:</p> <ul style="list-style-type: none"> • Passport • Personal ID card issued by the country of citizenship (for example, German <i>Personalausweis</i>, Belgian identity card, Italian <i>carta d'identita</i>) • Military ID card issued by one of the NATO Sending States (Belgium, Canada, France, the Netherlands, United Kingdom) <p>Item 10. Supporting document expiration date Enter the expiration date of the supporting document (for example, expiration date of passport or German <i>Personalausweis</i>).</p> <p>Item 11. Residence permit If required, check the appropriate box to indicate whether a copy of the residence permit is attached. See AE Reg 190-16 for guidance.</p> <p>Item 12. Work permit If required, check the appropriate box to indicate whether a copy of the work permit is attached. See AE Reg 190-16 for guidance.</p> <p>Item 13. Type pass requested Check the appropriate box. If an installation pass is desired, a temporary installation pass may be issued pending completion of a required background check. A temporary installation pass is valid for up to 90 days. The restrictions associated with each pass are different for each individual's access requirements.</p> <p>Item 19. Installations for which access is required Enter the level of access required. Depending on the person category, access may be restricted per AE Reg 190-16. Access should be limited to the least amount required. Examples include Taylor Barracks; 293d BSB (Mannheim); 26th ASG-wide; USAREUR-wide (Germany only).</p> <p>The following levels of USAREUR-wide access are available: USAREUR/USAFE-wide USAREUR-wide USAREUR/USAFE (Germany only) USAREUR (Germany only)</p> <p>NOTE: If liberal access is required, the sponsoring organization and the IACS registrar must take steps to ensure the proper selection from the above is made. For example, a contractor who operates exclusively within Germany should never be given USAREUR/USAFE-wide access.</p>	<ul style="list-style-type: none"> • DOD ID-card holder • Local national employee • Contractor (based in United States) • Contractor (living in host nation) • Personal-service employee • Delivery personnel (recurring deliveries or similar service not associated with a Government contract) • Vendor or commercial solicitor • NATO member • Host-nation military member 	<ul style="list-style-type: none"> • Foreign student (Marshall Center) • Member of private organization • Visitor (immediate family member living in Europe) • Visitor (friend or family member not included in category above) • Official guest • Department of State and American Embassy personnel • Other 	<p>Item 19. Installations for which access is required (continued) If any level of USAREUR-wide access is requested above, the sponsoring official must include a written justification in item 27. The written justification must demonstrate why the applicant requires the level of access in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to USAREUR/USAFE-wide access; no justification is required.</p> <p>Item 20. Limitations/time/day access is required Enter "24/7" if access is required all the time; otherwise state the specific days of the week and times. IACOs may require justification for liberal access (such as 24/7), so sponsoring organizations should be prepared to justify this entry.</p> <p>Item 21. FPCON restriction Enter the FPCON restriction. The IACS will establish a default FPCON according to AE Reg 190-16. Sponsoring officials may request a reduction or a one-FPCON increase.</p> <ul style="list-style-type: none"> • Delta • Charlie • Bravo • Alpha <p>Item 22. Pass expiration date Enter the desired installation pass expiration date. This field will be validated by the IACO. Justification for this date must be provided. A temporary installation pass is valid for up to 90 days. The expiration date of an installation pass depends on the limitations of the person category (item 7) selected as well as the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass. The expiration date will be whichever date is earlier.</p> <p>Item 23. Sign-in privileges Check the appropriate box to indicate whether sign-in privileges are required. If sign-in privileges are requested, the sponsoring official must include a written justification in item 28. The written justification must demonstrate why the applicant requires sign-in privileges in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to sign-in privileges authorized; no justification is required.</p> <p>Item 24. Privately owned vehicle (POV) registration information</p> <ol style="list-style-type: none"> a. State the license plate number exactly as it appears. b. State the country the license plate was issued for. c. State the make of the vehicle (for example, Opel, Saab, BMW). d. State the model of the vehicle (for example, 325i, Astra, 190E, S60). e. State the year of the vehicle (YYYY). f. State the body type of the vehicle (for example, 2-door sedan, bus). g. State the color of the vehicle. <p>Item 25. Company name and telephone number This item is only applicable for applicants in the Contractor (living in host nation) person category. If applicable, enter the name and telephone number of the company.</p> <p>Item 26. Verification by sponsoring official authority State the name, title, organization, and telephone number of the sponsoring official. The BSB IACO must have a copy of the designation of sponsoring officials memorandum from your organization identifying who is authorized to sign installation pass applications.</p> <p>Item 27. Installations for which access is required Enter the written justification that demonstrates why the applicant requires the level of access in the performance of duties.</p> <p>Item 28. Sign-in privileges Enter the written justification that demonstrates why the applicant requires sign-in privileges in the performance of duties.</p>
<ul style="list-style-type: none"> • DOD ID-card holder • Local national employee • Contractor (based in United States) • Contractor (living in host nation) • Personal-service employee • Delivery personnel (recurring deliveries or similar service not associated with a Government contract) • Vendor or commercial solicitor • NATO member • Host-nation military member 	<ul style="list-style-type: none"> • Foreign student (Marshall Center) • Member of private organization • Visitor (immediate family member living in Europe) • Visitor (friend or family member not included in category above) • Official guest • Department of State and American Embassy personnel • Other 		

Figure 2. Sample AE Form 190-16A (Continued)

- (3) To renew a pass that has expired or is about to expire (para 30).
- (4) To replace a pass that was lost or stolen (para 31).
- (5) To extend a Temporary Installation Pass (para 32).
- (6) To replace an unserviceable pass (para 33).

NOTE: Applications must be completed in English using standard American measurements. Figure 3 is a height and weight conversion chart.

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

(1) Sponsoring Organization. The sponsoring organization will designate individuals in its organization to take care of the sponsoring organization's responsibilities. The sponsoring organization for each applicant is based on the applicant's category (paras 12 through 27). For example, the BSB 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 civilian equivalent (GS-13) 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 rank or civilian pay-grade structure (for example, military banking facilities, Government travel agency), the local senior manager or deputy of the organization is authorized to sign the designation memorandum. Sponsoring organizations without a military rank or civilian pay-grade structure must ensure that the application does not authorize access beyond the BSB. Sponsoring organizations will ensure the organization's security manager delivers the sponsoring official designation memorandum (fig 4) 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 and to verify that the appropriate organization is listed as the sponsoring organization.

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

1. Supervisor in the rank of sergeant first class or chief warrant officer 2, or civilian pay grade of GS-9 or C-6A: authorized to sponsor individuals for only single-installation access.

2. Supervisor in the rank of first sergeant or master sergeant, chief warrant officer 3, captain, or civilian pay grade of GS-11, NF 4, or C-7: authorized to sponsor individuals for BSB access.

3. Supervisor in the rank of sergeant major, major, chief warrant officer 4, or civilian pay grade GS-12, NF 4, or C-7A: authorized to sponsor individuals for ASG access.

4. Supervisor in the rank of lieutenant colonel or civilian paygrade GS-13, NF 5, or C-8: authorized to sponsor individuals for U.S. Forces-wide access. Paragraph 15d provides additional restrictions for applicants in the Contractor (Living in Host Nation) category.

NOTE: The 22d ASG and 80th ASG 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. The PM will post this memorandum to the restricted portion of the IACS website, where it will be available to all USAREUR IACOs. IACOs will honor any memorandum posted to the IACS website, regardless of the requirements in (b) and (c) above.

**Weight-Conversion Chart:
(2.2045 pounds = 1 kg)**

Weight in kilograms	Converted to pounds
35	77
37	82
39	86
41	90
43	95
45	99
47	104
49	108
51	112
53	117
55	121
57	126
59	130
61	134
63	139
65	143
67	148
69	152
71	157
73	161
75	165
77	170
79	174
81	179
83	183
85	187
87	192
89	196
91	201
93	205
95	209
97	214
99	218
101	223
103	227
105	231
107	236
109	240
111	245
113	249
115	254
117	258
119	262
121	267
123	271
125	276
127	280
129	284
131	289
133	293
135	298
137	302

**Height-Conversion Chart
(.39370 inches = 1 cm)**

Height in centimeters	Height in feet and inches	Height in inches
122	4 feet 0 inches	48
124	4 feet 1 inches	49
127	4 feet 2 inches	50
130	4 feet 3 inches	51
132	4 feet 4 inches	52
135	4 feet 5 inches	53
137	4 feet 6 inches	54
140	4 feet 7 inches	55
142	4 feet 8 inches	56
145	4 feet 9 inches	57
147	4 feet 10 inches	58
150	4 feet 11 inches	59
152	5 feet 0 inches	60
155	5 feet 1 inches	61
157	5 feet 2 inches	62
160	5 feet 3 inches	63
163	5 feet 4 inches	64
165	5 feet 5 inches	65
168	5 feet 6 inches	66
170	5 feet 7 inches	67
173	5 feet 8 inches	68
175	5 feet 9 inches	69
178	5 feet 10 inches	70
180	5 feet 11 inches	71
183	6 feet 0 inches	72
185	6 feet 1 inches	73
188	6 feet 2 inches	74
191	6 feet 3 inches	75
193	6 feet 4 inches	76
196	6 feet 5 inches	77
198	6 feet 6 inches	78
201	6 feet 7 inches	79
203	6 feet 8 inches	80
206	6 feet 9 inches	81
208	6 feet 10 inches	82
211	6 feet 11 inches	83

Figure 3. Height and Weight Conversion Chart

Appropriate 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 U.S. Forces-wide access *(minimum LTC/GS-13/C-8/NF 5)*

FULL NAME	POSITION	RANK/GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	------------	-------------------------

b. Authorized to grant up to ASG-wide access *(minimum SGM/CSM/MAJ/CW4/GS-12/C-7A/NF 4)*:

FULL NAME	POSITION	RANK/GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	------------	-------------------------

c. Authorized to grant up to BSB-wide access *(minimum ISG/MSG/CW3/CPT/GS-11/C-7/NF 4)*:

FULL NAME	POSITION	RANK/GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	------------	-------------------------

d. Authorized to grant access for only one installation *(minimum SFC/CW2/GS-9/C-6A)*:

FULL NAME	POSITION	RANK/GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	------------	-------------------------

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 in the chain of command)

Figure 4. Format for Designation of Sponsoring Officials Memorandum

(e) Sponsoring officials will ensure the requirements and intent of this regulation are followed.

(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); IACO registrars will verify its correctness. The registration requirements and restrictions vary among categories.

(4) Type of Installation Pass Requested. Sponsors will request either the Temporary Installation Pass or 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. Background-check requirements are based on an individual's category. Sponsoring organizations are responsible for completing required background checks. IACO registrars will require verification that a background check has been completed or, when applicable, that a background check has been initiated. Sponsoring organizations should refer to the appropriate category (paras 12 through 27) to determine the exact background-check requirements for each applicant.

(b) Background checks that uncover no derogatory information will be forwarded to the sponsoring organization. Background checks that uncover derogatory information will be forwarded to the sponsoring organization and to the host ASG. The ASG will coordinate with the sponsoring organization to determine whether the derogatory information warrants denial of access privileges. If the requested access is for more than one ASG, the USAREUR PM must be consulted. When determining whether or not derogatory information should warrant denial of access privileges, ASGs and sponsoring organizations will consider both the seriousness of the derogatory information and when the incident or offense occurred.

(c) The following explains the types of background checks used for installation passes:

1. Police Good Conduct Certificate (*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.

2. MP Check. Sponsoring officials will obtain an MP-records check from their servicing MP station.

3. DCII. The DCII is the automated central repository that identifies investigations conducted by DOD investigative agencies and shows personnel security determinations made by DOD adjudicative authorities. The DCII database consists of an index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects in investigative documents maintained by DOD criminal, counterintelligence, fraud, and personnel-security investigative activities. DOD investigative and adjudicative authorities report information that is used for investigative, adjudicative, statistical, research, and other purposes as authorized. The DCII is only for individuals with social security numbers who have had affiliation with the U.S. Forces. Sponsoring officials may coordinate with their organization's security manager to determine the nearest DCII-access terminal.

4. FNS. The USAREUR PM uses the Foreign National Screening Program to ensure only suitable foreign nationals are granted access to installations. An FNS may also be conducted on U.S. citizens who have lived in Germany for an extended period. The USAREUR G2 manages this program. Sponsoring organizations will comply with FNS procedures in USAREUR Regulation 604-1. Documentation showing that the FNS has been initiated (required in some cases before issuing a Temporary Installation Pass) or that it has been completed may be obtained from the FNS website (<https://www.dcsintweb.hqusareur.army.mil/fnsp>). Questions about FNS should be addressed to the unit or organization security officer.

(d) It is not uncommon for an applicant to be ineligible to have a required background check completed because of the applicant's country of residence or length of time the applicant has lived in Germany. For instance, an applicant must have lived in Germany during the past 12 or more months for an FNS to be initiated. Applicants in the Vendor and Commercial Solicitor category who come from other countries to sell their merchandise often have this issue. Although a BSB has the authority to deny an installation pass based on its inability to conduct background checks and properly clear the applicant, BSBs should handle each situation individually and make a determination based on a risk assessment. BSBs 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 Police Good Conduct Certificate and require this document to be in English and notarized.

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

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

(6) Residence and Work Permits.

(a) As a rule, any non-German citizen may work for the U.S. Armed Forces in Germany if he or she has a residence permit (*Aufenthaltsberechtigung*, *Aufenthaltserlaubnis*, or *Aufenthaltsbewilligung*) and a work permit (*Arbeitslaubnis*).

(b) Installation-Pass applicants must have residence and work permits before receiving an Installation Pass unless the applicant is exempt from this requirement according to (d) below.

(c) If indicated in the registration requirements of the person's category, non-German citizens and contractors in Germany who work for DOD must submit a copy of their residence and their work permits. The residence permit is stamped in the passport. The work permit is issued on a separate form.

(d) Citizens of EU-member states are exempt from the work-permit requirement. They should, however, have an EU residence permit (separate form) if they have established their permanent residence in Germany. The following types of individuals are also exempt from the work-permit requirement:

1. Soldiers, members of the civilian component, and employees of organizations or contractors who have status under Articles 71 through 73, NATO Status of Forces Agreement (SOFA) Supplementary Agreement.

2. Non-German citizens who are family members of U.S. Armed Forces personnel or family members of personnel who are assigned to the civilian component.

3. Students at German universities coming from non-EU countries if they work less than 3 months during the university's vacation period. They must, however, have a residence permit.

(7) Number of Installations to Which Access Is Required.

(a) One of the main objectives of the Installation Access Control Program is to limit access to the minimum number of installations based on individual requirements.

(b) The following categories will be granted U.S. Forces-wide access in the USAREUR AOR without being required to provide justification:

1. DOD ID-Card Holder (para 12).

2. NATO Member (para 19).

3. Department of State and American Embassy Personnel (para 26).

(c) If justification is required for an individual to gain access to installations in the USAREUR AOR, the individual's sponsoring official will—

1. Ensure the application lists the minimum number of installations to which access is required by listing the specific name of the ASG, BSB, or installations (for example, only Taylor Barracks and Coleman Barracks, only 293d BSB). If access is required to more than one BSB or installation, provide detailed justification.

2. If an applicant in Germany requires "USAREUR-wide" access, indicate whether the requirement is only for Army installations or will include U.S. Air Force installations. Also, the application must specify whether access is required at the 22d ASG and 80th ASG. If access is required in the 22d ASG AOR, the application must include written permission from the 22d ASG PMO.

(d) If justification is required for an individual to enter installations in the USAREUR AOR, the IACO issuing official will—

1. Ensure the level of access requested does not exceed the sponsoring official's authority.

2. Clarify inadequate justifications by coordinating with the sponsoring official.

3. Carefully examine all applications for individuals under the Contractor (Living in Host Nation) category (para 15) to ensure the requested level of access meets requirements in paragraph 15.

(8) Days and Times Access Is Required. Sponsoring officials will ensure the application shows the minimum days and times access is required.

(9) Sign-in Privileges. Sponsoring officials may request sign-in privileges for the applicant only if bona fide justification is available. This justification must extend beyond 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 will be limited to other contractors and individuals on official business, not for personal business. The only exceptions are people in the NATO Member (para 19) and Department of State and American Embassy Personnel (para 26) categories, who receive automatic sign-in privileges.

(a) Installation-Pass holders with sign-in privileges will follow the sign-in procedures in paragraph 38.

(b) IACO registrars will ensure the rank and pay-grade requirements of the sponsoring official are met when sign-in privileges are requested for contractors in the Contractor (Living in Host Nation) category (para 15).

(c) Sign-in privileges will never be authorized for Temporary Installation Pass holders.

(d) People in categories with authorized sign-in privileges may sign in no more than four individuals and their vehicles.

(10) FPCON Restrictions. FPCON restrictions are based on an individual's category. The IACS will prohibit access beyond the FPCON associated with the category (paras 12 through 27). If sponsoring officials want to further restrict access at any of the FPCON levels, the application must specify the restriction.

(11) Vehicle Information. All individuals applying for an Installation Pass will register the vehicles they use to enter U.S. Forces installations in the USAREUR AOR. Only POVs are required to be registered and associated with an applicant's IACS record, not company vehicles. Proof of ownership is not required for the purpose of registering in IACS and will never be grounds to deny issuance of a regular or temporary pass. The following vehicle information must be included in blocks 24 and 25 of the application (AE Form 190-16A):

(a) License-plate number and country of issue.

(b) Make, model, year, body type, and color.

(c) Company's name and telephone number (only for Contractor (Living in Host Nation) category).

c. When the application is complete, the sponsoring official will escort the applicant to the servicing IACO with the required documentation (d 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 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.

(5) The applicant will take the signed original copy of the application to the servicing IACO and obtain an installation pass.

NOTE: Applicants will use similar procedures if they obtain access to the installation, but the sponsoring official is unable to escort them to the IACO. 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.

d. 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, United Kingdom).

(2) A copy of all required background-check results.

(3) Verification that the applicant has a residence permit and a work permit, if required.

NOTE: The applicant is not required to provide a photograph.

29. APPLICATION PROCEDURES FOR APPLICANT WITH TEMPORARY INSTALLATION PASS

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 FNS was completed.

c. If the notification is by e-mail, the IACO issuing official will verify that the e-mail is from an authorized sponsoring official by checking the memorandum designating sponsoring officials from the sponsoring organization (fig 4).

d. The IACO notification must include the date the FNS was completed and that the results include no derogatory information. If derogatory information is found, the notification must state that the host ASG 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 an Installation Pass. The notification paperwork will be filed with the original Temporary Installation Pass application packet.

30. APPLICATION PROCEDURES FOR RENEWAL PASS

a. Renewal requests must be submitted on a new application (AE Form 190-16A) from the sponsoring organization to validate the information on the original application.

b. The following applies to background checks when an applicant renews an Installation Pass:

(1) A new Police Good Conduct Certificate will be required if both of the following apply:

(a) A certificate was required based on the person's category. This requirement does not apply to people in the Local National Employee category (para 13).

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

(2) A new MP check will be required if one was initially required based on the person's category.

(3) A new DCII will be required if one was initially required based on the person's category.

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

c. Applicants will turn in the expiring or expired Installation Pass or receipt for it (if an MP official confiscated an expired pass) before receiving a new Installation Pass.

31. 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.

32. APPLICATION PROCEDURES FOR EXTENSION OF TEMPORARY PASS

a. A Temporary Installation Pass may be extended only once for no more than 90 days with reasonable justification. The primary intent of allowing an extension is to provide Temporary Installation Pass holders with continued access when there is an unforeseen delay in receiving FNS results. If the FNS returns with derogatory information that warrants denial of an Installation Pass, the Temporary Installation Pass holder will not be issued another Temporary Installation Pass. Background checks with derogatory information will be processed according to paragraphs 5c(4), 5e(4), 5i(2), and 5k(3).

b. The sponsoring official will coordinate with the IACO that issued the Temporary Installation Pass. After the extension is approved by the issuing official, the Temporary Installation Pass holder will return to the IACO, return the original Temporary Installation Pass, and obtain a new Temporary Installation Pass with a new expiration date.

c. If the reason for the extension request is a delay in the FNS results, the issuing official will coordinate with the USAREUR G2 to determine the FNS status.

d. This one-time extension will not be used to circumvent the more stringent requirements of an Installation Pass.

33. UNSERVICEABLE PASS

An unserviceable installation pass may be exchanged, one-for-one, at the pass holder's servicing IACO without action from the sponsoring organization. The pass holder will return the unserviceable installation pass unless the pass was confiscated by an MP official (para 41a(4)). If the pass was confiscated by an MP official, the receipt from the MP may be used to obtain a new pass. The expiration date will remain the same as that on the original installation pass.

SECTION V INSTALLATION ACCESS CONTROL OFFICE

34. 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/Resources/USAREURIACSRegistrationStations.pdf>.

b. With the exception of certain default settings in the IACS, IACOs have few limits on the type of installation passes that may be issued. For example, every IACO is authorized to issue a USAREUR-wide installation pass. This authority is based on the assumption that each IACO will follow the policy, procedures, and intent of this regulation and that the USAREUR PM will monitor the IACS activity.

c. Access control is an installation commander's responsibility. Organizations outside the direct control of the ASG and BSB will neither be authorized to issue installation passes nor will they be equipped with the IACS.

d. Authorized IACOs will be approved before the IACS is operational. Requests for additional IACOs or IACS-registration stations must be submitted through command channels to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

e. BSBs should functionally align their IACO under their servicing PMO.

f. IACO registrars will—

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

(2) Develop a system to conduct a 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) The plain, white plastic cardstock does not require any special security or accountability procedures.

(b) The installation-pass “security laminate” must be kept in a locked container in a cool, dry place when not in use. Incidents involving loss or theft of security laminate material from an IACO must be investigated promptly by the MP and reported to the USAREUR PM.

(c) IACO registrars will record the destruction of all installation passes or security laminate on a record-of-destruction memorandum and annotate the final disposition of passes in the IACS.

(d) IACOs will receive installation-pass cardstock and security laminate from the USAREUR PM. IACOs will keep an adequate stock of passes and laminate at all times.

35. REGISTRATION PROCEDURES FOR INSTALLATION-PASS APPLICANT

a. IACO registrars will process requests for installation passes as follows:

(1) Follow the procedures in paragraph 28c if the sponsoring official cannot accompany an applicant to the IACO. This will enable the applicant to enter the installation to obtain an installation pass.

(2) Verify that the sponsoring official is authorized to perform sponsoring-official duties by checking the sponsoring organization’s designation of sponsoring official memorandum that is on file. The issuing official will reject any application signed by an unauthorized sponsoring official.

(3) Receive the application and supporting documents from the applicant and reject any application that does not include required documentation. It is critical to the success of the Installation Access Control Program that registrars check the supporting documentation to minimize the potential of high-risk individuals obtaining access to U.S Forces installations in the USAREUR AOR.

(4) Register the applicant in the IACS with the information provided in the application. For restrictions that are subject to the sponsoring official’s written justification (for example, sign-in privileges, number of installations authorized), the registrar will clarify any justification that is insufficient as a quality-control check for the overall system. In particular, if “USAREUR-wide” access is requested, registrars will check to see whether a lower level of access would be more appropriate, such as “USAREUR-wide (Germany only).”

(5) Before giving the applicant the installation pass, ensure that the applicant signs and dates an installation-pass-holder Acknowledgement of Responsibilities memorandum (fig 5) and the Privacy Act statement (fig 6). The applicant should keep a copy of the memorandum. The Privacy Act statement is required only for U.S. citizens.

(6) File the completed application packet. A complete application packet will include the application (AE Form 190-16A), a copy of supporting documents, the original copy of the acknowledgement of responsibilities memorandum, the Print Summary Page from the IACS, and the signed Privacy Act statement (for U.S. citizens only). For Temporary Installation Pass holders receiving an Installation Pass, the issuing official will file the notification information with the original Temporary Installation Pass application packet.

b. Procedures for issuing an Installation Pass when an individual has a valid Temporary Installation Pass are in paragraph 29. Information on processing renewal applications, lost and stolen passes, extensions to Temporary Installation Passes, and unserviceable Installation Passes is in paragraphs 30 through 33.

MEMORANDUM FOR RECORD

SUBJECT: Acknowledgement of Installation-Pass-Holder Responsibilities

1. Reference AE Regulation 190-16, Installation Access Control, 19 October 2003.

2. As a USAREUR/USAFE 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 attempting to gain entry who refuse to identify themselves, provide digitized fingerprint minutia data (DFMD), or consent to search 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 military police (MP) official 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—

(1) It 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 MP or the 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.

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

(Print) Last, First, MI

Signature

Date

Figure 5. Sample Installation-Pass-Holder Acknowledgement of Responsibilities

36. REGISTRATION PROCEDURES FOR DOD ID-CARD HOLDER

To register a DOD ID-card holder, registrars will—

a. Verify the DOD ID-card holder's requirement to be registered in the IACS.

b. Register the DOD ID-card holder in the IACS.

c. File the signed and dated Privacy Act statement (fig 5).

PRIVACY ACT STATEMENT

AUTHORITY: Public Law 106-246, Title 10 USC, DODD 8500.1, AR 380-19, and EO 9397.

PRINCIPAL PURPOSE: To control local access to DOD information or information-based systems, and to control the physical access to installations, buildings, and controlled spaces by using measurable physical or behavioral characteristics to maintain accountability for issuance and disposition of installation passes.

ROUTINE USES: None. The “Blanket Routine Uses” are set forth at the beginning of the Army’s compilation of systems of records notices.

DISCLOSURE: Voluntary. Failure to provide the requested information may result in denial of access to DOD information-based systems, DOD facilities, or both.

By signing below, I acknowledge that I have read and understand the conditions set forth in the above Privacy Act statement.

Printed Name	Signature	Date
--------------	-----------	------

Figure 6. Privacy Act Statement

37. PROCESSING ACCESS ROSTERS

- a. Access-roster procedures are explained in paragraph 39.
- b. Access rosters will be processed through the servicing IACO unless an exception applies according to paragraph 39e(5).
- c. IACO registrars will—
 - (1) Ensure access rosters are prepared and processed according to paragraph 39.
 - (2) Use the access-roster module in the IACS to automate the access-roster system after the IACS is operational at the ACPs.

**SECTION VI
ACCESS PROCEDURES**

38. SIGN-IN PROCEDURES

Sign-in procedures will provide access to U.S. Forces installations in the USAREUR AOR if an access roster is unnecessary and issuing an Installation Pass is impractical or not authorized.

a. Sign-In Privileges.

- (1) DOD ID-card holders who are 18 years of age and older have sign-in privileges. If for some reason this privilege has been suspended, it will be shown only in the IACS, not on the DOD ID-card itself. If a DOD ID-card holder has sign-in privileges withdrawn, the only way a guard will know this is by checking the IACS at the ACP. DOD ID-card holders not registered in the IACS are not authorized sign-in privileges.
- (2) With the exception of individuals in the NATO Member and Department of State and American Embassy Personnel categories, Installation-Pass holders will not be granted sign-in privileges unless the sponsoring organization justifies the need. This action will be done during the IACS registration process. Sign-in privileges will be indicated 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. Temporary Installation Pass holders will not be authorized sign-in privileges.

b. Restrictions.

(1) Individuals under 18 years of age are not authorized sign-in privileges.

(2) Both DOD ID-card holders and Installation-Pass holders who are authorized sign-in privileges are limited to signing in four individuals and their vehicles at any one time. Using multiple sign-ins to circumvent this limit is prohibited.

(3) 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 Delta, only DOD ID-card holders will be authorized sign-in privileges.

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 the IACS, 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 will automatically display a warning message if this 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 up to the authorized limits (b(2) above). The IACS will automatically check the bar roster to ensure these individuals are not barred from the installation.

(3) If the ACP is not equipped with the IACS, the local SOP will provide procedures for accounting for signed-in individuals. The SOP for sign-in procedures should be as similar to those in (2) above as possible.

e. Sponsor Responsibilities. The sponsor will monitor the activity of individuals they sign in and be responsible for their conduct. Failure to follow sign-in policy and procedures may result in the withdrawal of sign-in privileges.

39. ACCESS ROSTERS

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

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

(1) Example 1: An authorized DOD ID-card holder requires four meetings with several LNs (not already 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 because the meetings are not regularly scheduled, are site-specific, and are not scheduled beyond 60 days.

(2) 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 22).

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

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

e. The following procedures must be conducted to process access rosters:

(1) Only DOD ID-card holders registered in the IACS may sign an access-roster request. IACO registrars will check the IACS to ensure the requester is a registered DOD ID-card holder.

(2) Original access-roster requests will be hand-carried to the servicing IACO or sent electronically from a .mil e-mail address that includes the name of the individual signing the access-roster request (for example, john.smith@us.army.mil). If the request is sent by e-mail, the IACO issuing official will confirm receipt. Access-roster requests may not be sent by fax. A complete list of IACOs is at <http://www.hqusareur.army.mil/opm/iacs/Resources/USAREURIACSRegistrationStations.pdf>.

(3) Access-roster requests will be submitted no less than 3 duty days before the desired effective date of the access roster to ensure IACO registrars have enough time to process the access roster.

(4) Access rosters will include the following information:

(a) Full name, country of citizenship, passport number or personal ID number (for example, the number from one of the documents listed in para 28d(1), 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, which may not be more than 60 days apart.

(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. For large-scale access-roster requests, such as one required to support the USAREUR Personal Property Shipment Program, the use of statements such as “USAREUR-wide” or “98th ASG-wide” is authorized. However, liberal access authorization like this should be avoided unless needed for operational requirements. The Installation Access Control Program limits access to the minimum number of installations to which access is required. Organizations will not use access rosters to circumvent the requirement to keep access to the absolute minimum simply for convenience.

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

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

(f) If an access roster is used for contract workers or vendors (for example, construction crew, contracted delivery services), a Police Good Conduct Certificate will be required and rules concerning residence and work permit requirements will apply. This documentation must accompany the access-roster request. If the request is sent by e-mail, the requester must indicate that the certificate has been received and permit requirements have been met.

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

(6) BSBs will establish procedures to ensure—

(a) Individuals on access-roster requests are screened against the 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 BSB before distribution.

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

f. The following procedures will be conducted by access-control guards:

(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 passport or personal ID card (must be one of the documents listed in para 28d(1)) and compare the number on this document with the number on the access roster. These numbers must match.

(2) Guards will deny access when the 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.

g. When the IACS is operational at BSB ACPs, the BSB 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 f above, except that they will conduct a manual look-up in the IACS instead of using a printed access roster.

40. EMERGENCY-VEHICLE AND PROTECTIVE-SERVICES-VEHICLE ACCESS

BSBs will use the following access procedures for emergency personnel and vehicles (for example, police, fire, ambulance, protective-services vehicles):

a. Access During Emergency Conditions.

(1) Plainly marked emergency vehicles (both U.S. and host-nation) with sirens on and lights flashing will not be unduly delayed.

(2) BSB commanders will coordinate with local host-nation emergency-service providers to establish notification procedures to use in case of an emergency. These procedures should include when the emergency-service provider first receives the emergency notification and where the BSB (for example, the MP station) first receives the emergency notification.

(3) BSBs may require emergency vehicles to come to a stop to allow guards an opportunity to identify the driver and occupants of the emergency vehicle, conduct a cursory inspection of the interior of the vehicle, and determine the location of the emergency. This stop should be conducted as quickly as possible (normally less than 10 seconds) and should be coordinated with emergency-service providers in advance to ensure providers understand the BSB access-control requirements under emergency conditions.

b. U.S. Forces Police. U.S. Forces police (MP, USAFE security forces) in marked MP vehicles and wearing a military uniform are not required to show ID. U.S. Forces police in civilian clothes (for example, MP investigators, Criminal Investigation Division agents) or in an unmarked vehicle will present proper ID and follow normal access-control procedures unless operating under emergency conditions.

c. Host-Nation Police.

(1) Host-nation police in marked police vehicles and wearing host-nation police uniforms are not required to show ID when entering U.S. installations.

(2) Procedures in subparagraph a above will be used for host-nation police operating under emergency conditions.

(3) When the circumstances in (1) above do not apply, host-nation police will be required to show some type of personal ID (for example, passport, *Personalausweis*, German *Polizeausweis*, which has a name and picture on it and one of the following titles on the front: *Polizei Dienstaussweis* (regular police); *Zoll-Polizei Dienstaussweis* (customs police); *Kriminal-Polizei Dienstaussweis* (criminal police)). The 22d ASG and 80th ASG should include a description of the host-nation police IDs in local SOPs. If there is any reason to doubt the validity of the ID or the reason for entry into the installation, the guard will call the servicing U.S. Forces police (for example, MP).

(4) Host-nation police who work on the installation with the U.S. Forces police may be issued an Installation Pass using the Official Guest category (para 25) to access the installation.

d. Fire Department Personnel. Fire department personnel who work for the U.S. Forces should be issued an Installation Pass using the Local National Employee category (para 13). Personnel from host-nation fire departments should enter U.S. Forces installations only during emergencies.

e. Ambulance Service Personnel. Ambulance service is provided by host-nation hospitals. Ambulances will normally enter installations under emergency conditions with the siren on and lights flashing. Ambulances will not be unduly delayed during an emergency (a above). Ambulances in Germany are well marked with some or all of the following words: Ambulance, *Krankenwagen*, or *Notarzt*. The 22d ASG and 80th ASG should include a description of the host-nation ambulances in their local SOPs.

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

g. 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) If ACP guards recognize the HAV and driver, they may choose not to stop the HAV and waive the vehicle and its occupants through the gate.

(3) Only HAV drivers will present their DOD ID card (no dispatch, license, or other documents). Exceptions to this requirement will be on an installation basis and approved by the ASG commander. The 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 attempt 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.

NOTE: BSB commanders may establish alternate procedures or modify these procedures based on the FPCON.

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 (not just the driver).

(3) Follow the sign-in policy and procedures in paragraph 38 and the access-roster policy and procedures in paragraph 39.

(4) Notify the MP if a DOD ID card or installation pass is expired or unserviceable. Guards may grant access to individuals who had their unserviceable DOD ID card or installation pass confiscated by the MP if the individual is registered in the IACS and is authorized access (g and h below). If the individual cannot be identified in the IACS, access will be denied unless an individual with sign-in privileges signs for the individual whose card or pass has been confiscated.

NOTE: Only an MP may confiscate DOD ID cards or installation passes. The MP 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. A receipt for a confiscated or expired DOD ID card or installation pass will never be used as an authorized access document.

b. If the IACS is unavailable for access verification, guards must be able to manually check access documents. A second form of 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). BSBs will include procedures for manually checking access documents in BSB 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. This will provide positive verification of access authorization for individuals carrying these access documents. Checking other documents (for example, a second form of ID or vehicle registration) is not necessary if the individual is registered in the IACS and access is authorized.

NOTE: The full potential of IACS can only be realized with consistent and complete use of the system.

d. If scanning reveals that an installation-pass holder is not registered in the IACS, guards should check the date of issue before notifying the MP. Same-day issues might not be in the IACS database. Local SOPs should provide procedures for granting access to individuals with an installation pass who may not be registered in the IACS. If, however, the date of issue is more than 1 day old, guards must coordinate with the servicing MP office. The MP will confiscate the installation pass and determine its validity.

e. Unless authorized by the BSB commander or higher authority, guards will not deny access to valid DOD ID-card holders who are not registered in the IACS. These individuals are normally on TDY, on temporary additional duty orders, or are new arrivals. Guards also will—

(1) Inform nonregistered DOD ID-card holders to register in the IACS as soon as possible.

(2) Log the entry of nonregistered DOD ID-card holders in the IACS to record their access. This requirement may cause a minor inconvenience for the DOD ID-card holder, which will encourage the cardholder to get registered in the IACS at the earliest opportunity. DOD ID-card holders requiring access to a U.S. Forces installation only for a short period (for example, a weekend softball tournament) normally will not be required to register in the IACS. If a DOD ID-card holder has registered in the IACS but the IACS database has not been updated, guards will treat the individual as a non-registered DOD ID-card holder.

(3) Check other ID documents (for example, a second form of ID or vehicle registration) according to local policy and SOPs.

NOTE: DOD ID-card holders not registered in the IACS are not authorized sign-in privileges.

f. BSB commanders will ensure special guard orders prescribe the procedures in subparagraph e above.

g. If a DOD ID card or installation pass will not scan properly in the IACS (for example, defective barcode) and the card or pass holder says that he or she is registered in the IACS, guards may verify registration by conducting a records search at the IACS workstation in the guard shack. DOD ID-card holders and installation-pass holders who are positively registered in the IACS will be granted access and instructed to immediately obtain a new DOD ID card or installation pass. When the record search reveals that the individual is not registered in the IACS, or the cardholder acknowledges that he or she is not registered in the IACS, guards will refer to subparagraph d above for installation-pass holders and subparagraph e above for DOD ID-card holders.

h. If a DOD ID-card holder or installation pass holder has forgotten his or her card or pass, BSB commanders may authorize guards to use the IACS manual look-up feature to authorize access as an alternative to denying access.

i. Employment as a contract security guard is not a basis for obtaining an installation pass. Contract guards will—

(1) Use their company ID badge to access the installation when access is not required beyond the immediate vicinity of the ACP.

(2) Use sign-in procedures or access rosters when access is required on a nonrecurring basis (for example, to participate in training).

(3) Apply for an installation pass using the Contractor (Living in Host Nation) category (para 15) if access on a recurring basis is required because of the individual's position or duty location.

(4) Register in the IACS to support the user-logon requirements of the IACS during guard duty at ACPs with an operational IACS. A guard does not need an installation pass to register in the IACS to perform user-logon requirements.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

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

5 USC 552a(b), Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

10 USC 3013, Secretary of the Army

10 USC 5013, Secretary of the Navy

10 USC 8013, Secretary of the Air Force

NATO Status of Forces Agreement Supplementary Agreement

DOD Directive 8500.1, Information Assurance (IA)

AR 380-19, Information Systems Security

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

Technical Manual 5-583-2, Security Engineering Concept Design

AE Regulation 190-1, Registering and Operating Privately Owned Motor Vehicles in Germany

AE Regulation 190-13, Army in Europe Physical Security Program

USAREUR Regulation 525-13, Antiterrorism/Force Protection: Security of Personnel, Information, and Critical Resources

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

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

SECTION II FORMS

SF 50-B, Notification of Personnel Action

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 489, Geneva Convention Identity Card for Persons Who Accompany the Armed Forces

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

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

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 USAREUR/USAFE Installation Pass

AE Form 600-700A, USAREUR Privilege and Identification Card

GLOSSARY

SECTION I

ABBREVIATIONS

1st PERSCOM	1st Personnel Command
AAFES-Eur	Army and Air Force Exchange Service, Europe
ACP	access-control point
AOR	area of responsibility
ASG	area support group
AST	area support team
BSB	base support battalion
CAC	Common Access Card
CPF	central processing facility
DCII	Defense Clearance and Investigation Index
DEERS	Defense Enrollment Eligibility Reporting System
DEROS	date eligible for return from overseas
DFMD	digitized fingerprint minutia data
DOD	Department of Defense
EU	European Union
FNS	foreign national screening
FPCON	force protection condition
G2	Deputy Chief of Staff, G2, USAREUR
HAV	heavy armored vehicle
IACO	installation access control office
IACS	Installation Access Control System
ID	identification
IMA-Europe	United States Army Installation Management Agency, Europe Region Office
JA	Judge Advocate, USAREUR
LN	local national
MIPR	military interdepartmental purchase request
MP	military police
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
PCS	permanent change of station
PM	Provost Marshal, USAREUR
PMO	provost marshal office
POC	point of contact
POV	privately owned vehicle
PR&C	purchase request and commitment
SEV	security-escort vehicle
SOFA	Status of Forces Agreement
SOP	standing operating procedure
TDY	temporary duty
TM	technical manual
USAREUR	United States Army, Europe

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 16 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-card holders; the remaining 15 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.

Foreign National Screening Program

A program managed by the USAREUR G2 that is designed to conduct background checks on non-U.S. citizens.

installation access control office

An office, normally at the base support battalion or area support team, that is authorized by the Provost Marshal, USAREUR, to register individuals into the Installation Access Control System and produce and issue installation passes.

Installation Access Control System

The personnel access-verification system that manages the Installation Access Control Program in the USAREUR area of responsibility.

probable cause

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

registrar

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

requester

A DOD identification-card holder who requests 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 16) and the two Visitor (paras 23 and 24) categories of the Installation Access Control System.

sign-in

A privilege granted to certain categories of individuals that allows them to escort visitors after signing them on to an installation.

sponsoring official

An individual who represents the sponsoring organization and carries out the organization's sponsoring responsibilities. Sponsoring officials must be designated in writing.

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 access U.S. Forces installations. Every installation-pass applicant and installation-pass holder has a sponsoring organization.

unserviceable

Any condition or change to a DOD identification 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, print fading, or other deficiencies that do not impair the guard's ability to verify that the card or pass holder is the individual indicated.