

Department of the Army
US Army Garrison Schweinfurt
Schweinfurt, Germany 09033
01 June 2012

Emergency Services

Installation Access Control

Summary. This regulation prescribes policies procedures and responsibilities for the United States Army Garrison Schweinfurt (USAG Schweinfurt) Installation Access Procedures. It defines the four authorized Access Methods and responsibilities of sponsoring officials supporting agencies.

Applicability. This regulation applies to all Soldiers, Family members, Department of Defense (DOD) employees and is applicable to all individuals with legitimate need to access United States Army Garrison (USAG) Schweinfurt installations.

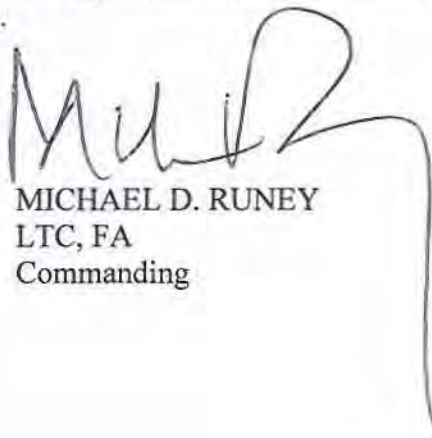
Supplements. Supplements to this regulation are prohibited without prior approval from the Director of Emergency Services (DES).

Interim Changes. Interim changes to this regulation are not official unless the DES authenticates them. Users will destroy on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. This regulation's proponent agency is USAG Schweinfurt and users are invited to send comments to the USAG Schweinfurt, ATTN: Emergency Services, APO AE 09033.

Distribution. This regulation is distributed through USAG Schweinfurt DES.

Forms. This regulation prescribes AE Form 190-16A, AE Form 190-16B, AE Form 190-16C, AE Form 190-16E, and AE Form 190-16F. AE and higher level forms are available through the Army in Europe Publishing System (AEPUBS).



MICHAEL D. RUNEY
LTC, FA
Commanding

Table of Contents

CHAPTER 1.....	<u>Para</u>	<u>Page</u>
GENERAL		
REFERENCES.....	1	3
PURPOSE	2	3
EXPLANATION OF ABBREVIATIONS AND TERMS.....	3	3
RESPONSIBILITIES.....	4	3
COMMANDER'S INTENT.....	5	7
PROCEDURES.....	6	7
EXCEPTIONS TO POLICY.....	7	13

APPENDIX LIST

APPENDIX A	INSTALLATION PASS APPLICATION EXAMPLE	A
APPENDIX B	ACCESS ROSTER APPLICATION EXAMPLE	B
APPENDIX C	SPONSORING OFFICIAL MEMORANDUM EXAMPLE	C
APPENDIX D	ADDITIONAL COUNTRY GUEST WORKSHEET	D

CHAPTER 1 GENERAL

1. References.

- a. Army Regulation (AR) 27-10, Military Justice
- b. AR 190-22, Search and Seizure
- c. AR 190-56, The Army Civilian Police and Security Officer Program
- d. Army in Europe Regulation (AER) 190-13, The USAREUR Physical Security Program
- e. AER 190-16, Installation Access Control
- f. AER 525-13, Antiterrorism/Force Protection
- g. AER 600-700, Identification Cards and Individual Logistical Support
- h. AER 27-9, Misconduct by Civilians
- i. AER 604-1, Foreign National Screening Program

2. Purpose. This policy is intended to supplement AER 190-16 with local procedures and guidelines not specifically covered in the basic regulation.

3. Explanation of Abbreviations and Terms. Abbreviations and terms are defined in the glossary of AER 190-16.

4. Responsibilities

- a. IRG Commanders will—

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

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

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

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

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

1. Instructions for sign-in procedures, access rosters, emergency and protective services vehicles, and processing nonregistered DOD ID cardholders.
2. Instructions for handling unique access requests not covered by this regulation.
3. Instructions for conducting manual checks of access documents if IACS operations are disrupted.

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

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

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

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

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

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

b. USAG Directors of Emergency Services (DESS) will—

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

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

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

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

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

(3) Develop procedures to ensure sponsoring organizations include the following information on all purchase requests and commitments (PR&Cs), military interdepartmental purchase requests (MIPRs), and other requests for contracting support when the contract will result in contractors requiring access to U.S. Forces installations:

(a) The name of the requiring activity and the name and telephone number of the requiring activity's installation-access POC.

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

d. IACO registrars will—

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

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

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

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

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

e. Sponsoring organizations will ensure—

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

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

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

(4) The applicant registers his or her privately owned vehicle (POV) according to the procedures in this regulation and AE Regulation 190-1 (when applicable). Vehicle registration is required for all installation-pass applicants who use a POV to enter U.S. Forces installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) Immediately report a lost or stolen DOD ID card or installation pass to the local military police office or servicing IACO so that the card can be deregistered.

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

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

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

5. Commander's intent: This policy outlines the requirements and procedures for installation access control within USAG Schweinfurt. Changes in the baseline force protection posture within USAG Schweinfurt may warrant changes to this policy to ensure the security of our installations as this regulation only covers up to and including FPCON Bravo. This policy does not apply to restricted areas governed by other regulations.

6. Procedures

a. Installation access within USAG Schweinfurt will be strictly enforced. This policy will not be supplemented without approval of the Garrison Commander. AER 190-16 Installation Access Control is the proponent for this policy. This policy is intended to supplement AER 190-16 with local procedures and guidelines not specifically covered in the basic regulation. The procedures of this policy will —

(1) Mandate the compliance with force protection condition (FPCON) measures related to access control.

(2) Prohibit the unlawful introduction of weapons, explosives, and/or other contraband onto our installations.

(3) Facilitate the identification of barred individuals and individuals who do not have a need or are not entitled to access our communities.

(4) Assist in the prevention of wrongful appropriation and pilferage of government property.

(5) Incorporate the IACS into provisions of this policy.

(6) Ensure the safety and security of US Forces personnel and property.

b. The USAG Schweinfurt Directorate of Emergency Services (DES) will:

(1) Serve as the proponent for all policy matters pertaining to access control.

(2) Conduct staff assistance visits and command inspections to ensure IACS registration and installation pass procedures are adhered to.

(3) Ensure all IACOs comply with regulatory requirements.

(4) Outline procedures to allow access for emergency vehicles if they differ from the requirements outlined in AER 190-16.

(5) Outline procedures for access of various types of vehicles and personnel at the various force protection conditions.

c. School buses: All school bus drivers must have a valid installation pass for access to the installation. School bus drivers will vouch for all students on the bus. Drivers that do not have a valid installation pass must be escorted to and from the pickup/drop-off location on the installation by a Department of Defense Education Activity contract bus representative. School busses with a security attendant on board do not need to be inspected to access the installation however they can still be inspected based on the current Random Antiterrorism Measure Program (RAMP).

d. Tour buses: For unaccompanied installation access, the bus driver, upon initial entry to an installation (first pick-up) for an authorized tour, will produce a manifest which lists the time, date, and location of personnel pickup. In the event that a bus arrives from another location, all occupants will present valid/authorized identification at the access control point. Security officers will check the valid/authorized identification, of each passenger.

e. Government shuttle buses: Shuttle bus drivers will vouch for all occupants on the bus.

f. Diplomatic vehicles: Vehicles with US diplomatic plates will be allowed access after the driver produces a valid access document as outlined in AER 190-16. Passengers will not be required to produce identification. The vehicle will not be searched.

g. Rental vehicles: Personnel desiring access to installations driving rental cars will be required to show their rental contract in addition to their valid Department of Defense identification card (DOD ID) card.

h. Military convoys: The convoy commander will remain at the access control point and vouch for the vehicles and personnel within the convoy. This will negate the requirement for security personnel to physically check every person in the convoy.

i. Physical training or military formations (five or more personnel): One person with a valid registered DOD ID card can vouch for the group of individuals within the main body of the formation. Individual runners and small groups (four or less personnel) must present valid DOD ID cards to gain access to the installation.

j. USAG Schweinfurt community members/guests:

(1) Each directorate will appoint a primary and alternate sponsoring official for installation access control and provide a copy of the appointment to the DES. Directorates may also appoint contracting officer representatives as sponsoring officials. Sponsorship must be kept to a minimum. Authorized sponsor exceptions must be approved by the Garrison Commander or the Deputy to the Garrison Commander.

(2) Individuals that may have access to our installations are:

(a) DOD ID Card holder

(b) DOD Installation pass holder

(c) Personnel on a DES approved access roster

(d) Personnel signed in by a DOD ID Card holder or installation pass holder with sign in privileges.

(3) DOD ID card holders are authorized to place individuals on the access roster. An individual who is placed on the access roster may not exceed 60 days in a 12 month period.

(4) DOD ID card holders and installation pass holders with sign-in privileges at the access control point (ACP) are only permitted to have four guests signed into the system at any time. An individual may not have more than four visitors signed into the IACS at any given time. The individual being signed in will present a valid form of identification (passport or *Personalausweis*) at the ACP to ensure the individual is not barred prior to being entered as a guest in the IACS. Guest will be escorted at all times by a trusted agent (ID card or installation pass holder) to include returning to the ACP to sign out. Contractors do not have to be signed

out by the same person that signed them in but the escort must be a trusted agent. Failure to sign your guest out may conflict with future sign-in.

(5) Personnel will not be signed in as guests for more than a 24 hour period as directed by the Garrison Commander. If the visit is expected to exceed 24 hours, both the sponsor and guest(s) will report to a USAG Schweinfurt ACP and the sponsor will sign their guest(s) out and then back in. Failure to return to the ACP and sign out will result in the guest being barred from all USAG Schweinfurt installations and a 30-day loss of sign-in privileges for the individual who signed the visitor in. A second offense will result in a 60-day loss of sign-in privileges. A third offense will result in a permanent revocation of sign-in privileges. Prior to signing-in a guest, the guest and sponsor will be required to read and acknowledge understanding of these control measures. The security guard performing the sign-in will be responsible for ensuring this occurs. Violators of the 24 hour sign-in period will be subject to administrative or judicial actions under the UCMJ or Civilian Misconduct Action Authority for Article 92, Failure to Obey a Lawful Order.

(6) Signing in of underage persons/minors:

(a) A minor is any person between the age of 10 and 17. Children under age 10 do not need to provide ID documentation to be allowed access to the installation. An individual under the age of 18 can be signed onto the installation when:

(1) The sponsor can reasonably explain the intent for the visit is one that will not violate law nor endanger the health, welfare or safety of the child. Juvenile curfew hours will be enforced when appropriate. For overnight visits in Government quarters the MP desk will be notified. Children will not be taken to soldier barracks unless escorted by a verifiable parent or legal guardian who gives their consent. Verifiable means that the adult in charge of the minor can reasonably demonstrate their authority to give consent. For example, the names match on the *Personalausweis* or the address is the same on identification documents or paperwork is provided that appoints the person as such.

(2) The sponsor (the ID card holder signing in the minor) is accompanied by a spouse or a family member as defined below.

(b) For the purpose of this guidance, the definition of a family member is limited to a son, daughter, parents, brothers, sisters, mother-in-law, father-in-law, brothers-in-law, sisters-in-law, grandparents, and grandparents-in-law.

(c) The intent of this guidance is to mitigate the potential risk of illegal activity. To ensure that members of the community, family or friends, are not unduly denied access, exceptions to this section may be obtained from the USAG Schweinfurt Provost Marshal Office.

(7) ACP procedures:

(a) Search authorization: Any vehicle or person attempting to access a USAG Schweinfurt installation is subject to search IAW AR 190-22 and USAREUR Suppl 1 to AR 190-22.

(b) Access to installations not authorized: IAW AER 190-16, Para 8a(2)(c), personnel in possession of a valid DOD installation pass may obtain access to an installation for which they are currently not authorized by producing either temporary duty (TDY) orders or a memorandum signed by the chief or deputy of their division.

(c) Forgotten ID Cards: Contract security officers at the ACP will verify that the individual is authorized access to the installation by performing a manual look-up to verify that the individual requesting access is a valid DOD ID card or installation pass holder.

(d) All DOD ID cards and installation passes that are expired will be confiscated by contract security officers or Military Police. ID cards or installation passes that are mutilated have illegible identification data or an unrecognizable photo will also be confiscated if the officers cannot positively verify that the individual matches the picture on the ID.

(e) An individual that has their ID card or installation pass confiscated will be issued a receipt by the Military Police or contract security officer when their card is confiscated. This receipt IS NOT an access document.

(f) Confiscated installation passes and ID cards will be turned in to the ID card section or IACO within 24 hours.

(g) Individuals who have their pass or ID card confiscated must be signed in as a visitor until a new pass or ID card is issued.

(h) When an individual fails to comply with this directive or objects with an order to surrender the expired or damaged ID card or installation pass, the Military Police will be notified.

(i) When trusted traveler procedures are utilized to maintain constant traffic flow, priority will be given to vehicles attempting to enter the installation over individuals manually signing in or out.

(8) Installation Passes:

(a) The DES is the USAG Schweinfurt staff proponent for installation passes and works in coordination with the DPTMS security manager to ensure this program is managed under the guidelines of the Local National Screening Program (LNSP). In regards to the categories listed in AER 190-16, USAG Schweinfurt has added the following category requirements when submitting an application:

1. Official Guest Category – Police Good Conduct Certificate, AE Form 604-1B and entered into the Local National Screening Program.

2. Visitor Category (Residing in Europe) AE Form 604-1B and entered into the Local National Screening Program.

3. Other Category – Police Good Conduct Certificate, AE Form 604-1B and entered into the Local National Screening Program.

4. Delivery Drivers – Installation Passes should be initially issued for 6 months and only when accompanied by the service owner. Drivers who have established themselves in the community through years of service without incident may receive renewals for 1 year. Owners must supply the IACS office copies of the business license and food preparation health certificate. Taxi drivers may be issued a pass for two years.

(b) Sponsors for installation passes will:

1. Ensure that a benchmark is set for Official Guest Category, i.e., active membership in a German/American Club or organization, regular participation in the organization, and individual is promoting good German/American relationships.

2. Ensure that privileges for installation passes are limited; United States Army Europe (USAREUR) wide access is not a blanket authorization and must be justified only those installations where the individual has a need to access will be listed. The week days identified on the pass will be limited to days of the week the individual must have access to the installation, i.e., few contractors do any business on the installation on Sundays. The access times will be restricted to only those times that the individual has to conduct business on the installation. The general rule for contractors will be Monday through Saturday from 0500 – 2200 hours.

3. Installation passes for transportation purposes will be approved by the sponsoring USAG Schweinfurt staff IACO before being processed.

4. Installation pass holders granted sign-in privileges are for official business only and limited to four persons with their vehicles. Persons granted sign-in authority should either be in a supervisory position or have an official need to ensure mission accomplishment (i.e. contracting officer representative project manager, etc.).

5. Individuals who abuse their installation pass privileges, i.e., use their installation pass as a means to access the installation for purposes other than the intent of the installation pass, will have their installation pass revoked. ID card and installation pass holders who abuse the sign-in privilege, i.e., the guest is unescorted, the guest does not sign-out, may have their sign-in privileges revoked.

k. State Sponsors of Terrorism. Citizens from countries identified by the United States Department of State (http://travel.state.gov/visa/temp/info/info_1300.html) require USAG Schweinfurt commander approval for USAG Schweinfurt access, and USAG Schweinfurt commander and USAREUR PM approval for Army-in-Europe wide access. The United States Department of State requires additional screening for citizens from identified countries before

they are granted entry into the United States (Immigration and Nationality Act (8 USS. 1101(a)(15) and Section 306 of the Enhanced Border Security and Visa Reform Act of 2002). Citizens from countries identified by the United States Department of State as state sponsors of terrorism who have previously been issued an installation pass are exempt from the requirement to obtain USAG Schweinfurt commander's approval for access.

l. The Garrison commander reserves the right to request additional information from any person requesting access to any USAG Schweinfurt installation.

7. Exception to Policy

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

b. Persons requesting an exception to any policy or procedure in this regulation must send their request through appropriate command channels to the USAREUR PM

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

Appendix A

APPLICATION FOR U.S. FORCES IN EUROPE INSTALLATION PASS (AE Reg 190-16)					
PRIVACY ACT STATEMENT (For U.S. Citizens)					
Authority: 5 USC 301 Departmental regulations; 10 USC 113, Secretary of Defense, Note at Pub. L. 106-65; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 18 USC 1029, Access Device Fraud; 18 USC. 1030, Computer Fraud; 40 USC Information Technology Management; 50 USC, Chapter 23, Internal Security; Pub. L. 103-398, Government Information Security Act; Pub. L. 100-235, Computer Security Act of 1987; Pub. L. 99-474, Computer Fraud and Abuse Act; EO 9397 (SSN).					
Principal purpose(s): To identify personnel authorized routine or recurring access to installations under U.S. control.					
Routine use(s): Those permitted under 5 USC 522a(b) of the Privacy Act and as specifically allowed outside the DOD pursuant to 5 USC 522a(b)(3) of the Privacy Act.					
Disclosure: Voluntary; however, failure to provide any item of information will result in denial of entry onto U.S.-controlled installations.					
<i>Please refer to the instructions on page 3 to ensure that the form is correctly filled in.</i>					
1. To USAG SCHWEINFURT DES		2. From		3. Date (YYYYMMDD)	
4. Name (Last, first, MI)		5. Sponsor address		6. Address (Company, organization, unit)	
7. Person category		8. Country of citizenship		9. Personal ID number	
10. Supporting document expiration date (Passport/ID card)		11. Residence permit required? <input type="checkbox"/> Yes <input type="checkbox"/> No		12. Work permit required? <input type="checkbox"/> Yes <input type="checkbox"/> No	
13. Type pass requested <input type="checkbox"/> Installation pass <input type="checkbox"/> Temporary installation pass		14. Date of birth (YYYYMMDD)	15. Weight (Pounds)	16. Height (Inches)	17. Eye (Color)
18. Hair (Color)		19. Limitations/time/day access is required			
				20. Pass expiration date (YYYYMMDD)	
IACO REGISTRAR MUST VALIDATE					
21. FPCON restriction		Justification (Refer to instructions page for justification requirements.)			
22. Installations for which access is required (Provide justification)					
Justification					
23. Sign-in privileges					
<input type="checkbox"/> No		<input type="checkbox"/> Yes (Provide justification)			
Justification					

Appendix A (Continued)

24. Privately owned vehicle (POV) registration information (Additional vehicles may be added on a separate sheet of paper)						
a. License number	b. Country	c. Make	d. Model	e. Year	f. Body type	g. Color
25. Company name, telephone number, and e-mail						
26. Required attachments (Check applicable boxes)						
All installation-pass applications must include supporting documents. Requirements may be different depending on the person category selected.						
<input type="checkbox"/> Residence Permit			<input type="checkbox"/> Fax-Back (U.S. contractor)			
<input type="checkbox"/> Work Permit			<input type="checkbox"/> Proof of AE Form 604-1A, Local National Screening Program (LNSP, Initiation)			
<input type="checkbox"/> Police Good Conduct Certificate (PGCC) (Polizeiliches Führungszeugnis) (no entries)			<input type="checkbox"/> LNSP (No entries)			
<input type="checkbox"/> PGCC (Entries adjudicated)			<input type="checkbox"/> LNSP (Entries adjudicated)			
<input type="checkbox"/> Military Police (MP) check						
27. Verification by sponsoring official (must check both boxes)						
<input type="checkbox"/> I have reviewed the results of all background checks required by AE Regulation 190-16 and verify that there is no derogatory information that would preclude the issuing of an installation pass.						
<input type="checkbox"/> I verify that the applicant has been informed about the purpose and proper use of the installation pass. I have reviewed AE Regulation 190-16 and believe this packet is administratively correct and fully and accurately indicates the applicant's access requirements. However, if there is a problem or you need further information, please contact me.						
a. Organization, telephone number, and e-mail			b. Name and title			
c. Signature (Digital or original)			d. Date (YYYYMMDD)			
28. To be completed by the registrar						
a. Registrar name (Printed)			b. IACS office			
c. Registrar's signature			d. Date issued (YYYYMMDD)			
29. Additional comments						

Appendix A (Continued)

Instructions for completing AE Form 190-16A			
<p>Block 1. To Enter the name of the servicing installation access control office.</p>	<p>Block 20. 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 (block 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>Block 2. From Enter the name of the sponsoring official's organization.</p>	<p>Block 21. FPCON restriction Enter the FPCON restriction. <ul style="list-style-type: none"> • Delta (provide justification, including first-responder duties) • Charlie (provide justification, including a list of essential duties) • Bravo </p>		
<p>Block 5. Sponsor address Enter the mailing address of the sponsoring organization. For the person categories Personal-Service Employee, Visitor (FM/Europe), and Visitor (not FM/Europe) also include the requester's mailing address.</p>	<p>Block 22. Installations for which access is required Sponsor must provide specific justification for applicant's access requirements in block 22. Access is limited to the minimum number of installations required for the applicant. Examples include Campbell Barracks or Taylor Barracks. If greater access is required (for example, USAG-wide, multiple USAGs, or access to an Air Force base or a Navy base), additional documentation is required, such as a contract statement of work that lists by name the installations and bases.</p>		
<p>Block 6. Address Enter the address of the unit 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>Block 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 block 23. The written justification must explain 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>Block 7. Person category</p> <table border="0"> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> » Contractor (EU/NATO) Contractor who is a resident of the European Union or a NATO-member country. » Contractor (U.S.) Contractor who is a U.S. citizen working for a U.S. company based in the United States. » Delivery Personnel Personnel making recurring deliveries or providing similar service not associated with a Government contract. » DOS/American Embassy Department of State and American Embassy personnel. » Foreign Student Foreign student at the Marshall Center. » Gate Guard » HN Government Host-nation Government official. </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> » HN Military Member Host-nation military member. » Local National Employee » Member PO Member of a private organization. » NATO Member » Official Guest » Personal-Service Employee » Vendor Vendor providing merchandise or services not associated with a Government contract. » Visitor (FM/Europe) Immediate Family member living in Europe. » Visitor (not FM/Europe) Friend or Family member not included in category above. » Other </td> </tr> </table>	<ul style="list-style-type: none"> » Contractor (EU/NATO) Contractor who is a resident of the European Union or a NATO-member country. » Contractor (U.S.) Contractor who is a U.S. citizen working for a U.S. company based in the United States. » Delivery Personnel Personnel making recurring deliveries or providing similar service not associated with a Government contract. » DOS/American Embassy Department of State and American Embassy personnel. » Foreign Student Foreign student at the Marshall Center. » Gate Guard » HN Government Host-nation Government official. 	<ul style="list-style-type: none"> » HN Military Member Host-nation military member. » Local National Employee » Member PO Member of a private organization. » NATO Member » Official Guest » Personal-Service Employee » Vendor Vendor providing merchandise or services not associated with a Government contract. » Visitor (FM/Europe) Immediate Family member living in Europe. » Visitor (not FM/Europe) Friend or Family member not included in category above. » Other 	<p>Block 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.
<ul style="list-style-type: none"> » Contractor (EU/NATO) Contractor who is a resident of the European Union or a NATO-member country. » Contractor (U.S.) Contractor who is a U.S. citizen working for a U.S. company based in the United States. » Delivery Personnel Personnel making recurring deliveries or providing similar service not associated with a Government contract. » DOS/American Embassy Department of State and American Embassy personnel. » Foreign Student Foreign student at the Marshall Center. » Gate Guard » HN Government Host-nation Government official. 	<ul style="list-style-type: none"> » HN Military Member Host-nation military member. » Local National Employee » Member PO Member of a private organization. » NATO Member » Official Guest » Personal-Service Employee » Vendor Vendor providing merchandise or services not associated with a Government contract. » Visitor (FM/Europe) Immediate Family member living in Europe. » Visitor (not FM/Europe) Friend or Family member not included in category above. » Other 		
<p>Block 9. Personal ID number Enter the personal ID number or the passport number from the supporting document used. The 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>Block 25. Company name, telephone number, and e-mail This block is applicable only for applicants in the Contractor (EU/NATO) person category. If applicable, enter name, telephone number, and e-mail of the company.</p>		
<p>Block 10. Supporting documentation expiration date Enter the expiration date of the supporting document (for example, expiration date of passport or German <i>Personalausweis</i>).</p>	<p>Block 26. Required attachments Check all applicable boxes and provide a photocopy of supporting documents.</p>		
<p>Block 11. Residence permit required? If required, check the appropriate box to indicate whether a copy of the residence permit is attached. See AE Regulation 190-16 for guidance.</p>	<p>Block 27. Verification by sponsoring official State the name, title, organization, telephone number, and e-mail of the sponsoring official. The 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>Block 12. Work permit required? If required, check the appropriate box to indicate whether a copy of the work permit is attached. See AE Regulation 190-16 for guidance.</p>	<p>Block 29. Additional comments Provide any requested information/justification.</p>		
<p>Block 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>Block 19. 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>			

FOR OFFICIAL USE ONLY

INSTALLATION ACCESS CONTROL SYSTEM (IACS) ACCESS-ROSTER REQUEST (AE Reg 190-16)	
Data required by the Privacy Act of 1974 (For U.S. citizens)	
<p>Authority: 5 USC, 301 Departmental Regulations; 10 USC 113, Secretary of Defense, Note at Pub. L. 106-65; 10 USC 136, Under Secretary of Defense for Personnel and Readiness; 18 USC 1029, Access Device Fraud; 18 USC 1030, Computer Fraud; 40 USC, Information Technology Management; 50 USC, Chapter 23, Internal Security; Pub. L. 106-398, Government Information Security Act; Pub. L. 100-235, Computer Security Act of 1987; Pub. L. 99-474, Computer Fraud and Abuse Act; E.O. 9397 (SSN).</p> <p>Principal purpose(s): To identify personnel authorized routine or recurring access to installations under U.S. control.</p> <p>Routine use(s): Those permitted under 5 USC 522a(b) of the Privacy Act and as specifically allowed outside the DOD pursuant to 5 USC 522a(b)(3) of the Privacy Act.</p> <p>Disclosure: Voluntary; however, failure to provide any item of information will result in denial of entry onto U.S.-controlled installations.</p>	
Instructions	
<ul style="list-style-type: none"> • Access-roster requests may be hand-carried or sent by e-mail from an official e-mail account (for example, .aafes.com, .eu.dodea.edu, .gov, .mil, .nato, .org). • Only DOD ID cardholders registered in the IACS may sponsor an access-roster request. • Access-roster requests must be submitted 3 workdays before the date access is needed. • Contractors and vendors must submit a copy of their passport/<i>Ausweis</i> and, if required, a visa/work permit along with a copy of a German Police Good Conduct Certificate (PGCC) or their country's equivalent (if not in English, translated by a certified translator). This may not be more than 12 months old. • U.S.-based contractors must submit a copy of a confirmed "fax-back." For more information about the fax-back process, please contact the DOD Contractor Personnel Office, Office of the Deputy Chief of Staff, G1, HQ USAREUR, at DSN 375-2518 or http://www.per.hqusareur.army.mil/cpd/docper/tdy_faxback.aspx. • Individuals may be placed on an access roster for up to 60 days. • For additional information on access rosters, refer to AE Regulation 190-16. 	
Sponsor Information	Access Roster Information
Last name: _____	Effective date (YYYYMMDD): _____
First name: _____	Expiration date (YYYYMMDD): _____
SSN (last four digits): _____	Reasons for access: _____ _____ _____
Date of birth (YYYYMMDD): _____	
E-mail: _____	
Work telephone number: _____	
Home or cell phone number: _____	
Unit or organization: _____	Installation for which access is authorized: _____ _____
To Be Completed for Contractors and Vendors Only	
Company name: _____	
Company e-mail and telephone: _____	
Days of week access is required: _____	Times of day access is required: _____
Copy of background check and work permit provided (if required) (non-U.S. citizen): Yes <input type="checkbox"/> No <input type="checkbox"/> On file at IACS office <input type="checkbox"/>	Copy of fax-back provided (U.S. citizen working for U.S. company): Yes <input type="checkbox"/> No <input type="checkbox"/> On file at IACS office <input type="checkbox"/>

Appendix C

LETTERHEAD

Office Symbol

Date

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

SUBJECT: Designation of Sponsoring Officials

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

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

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

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

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

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

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

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

FULL NAME POSITION GRADE OFFICIAL E-MAIL ADDRESS

SIGNATURE _____

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

Appendix C (Continued)

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

Format for Designating Sponsoring Officials

Appendix D

USAG SCHWEINFURT SPONSOR/GUEST SIGN-IN AGREEMENT

I, _____,
 Name (First, Last, MI) (Print) Rank/Last 4 of SSN or Id # Address, Unit, Bldg # Phone # of quarters or Cell #

hereby acknowledge and understand that:

- I am responsible for my guest's(s') conduct during his/her (their) entire visit.
- My guest(s) is (are) not authorized to leave the installation without being signed out.
- The visit will not exceed 24 hours from the date and time at which I signed in the guest(s).
- Upon completion of my guest's(s') visit, I must ensure that each of my guests returns, accompanied by either myself or some other person with sign-in privileges, to be signed out properly.
- Failure to comply with any of the above visitor sign-in policies and procedures may result in the revocation of my Visitor Sign-In Privileges for a period of up to 30 days for the first offense and 60 days for the second consecutive offense and permanently for the 3rd offense.

LAST NAME FIRST NAME SSN/PIN TELEPHONE NUMBER

GUEST #1: _____
 GUEST #2: _____
 GUEST #3: _____
 GUEST #4: _____

Purpose of visit	Requested destination(s)
------------------	--------------------------

Vehicle Plate Number(s)	Vehicle Make	Model	Color (s)
-------------------------	--------------	-------	-----------

 Signature of Sponsor Date Time

Guest(s) Acknowledgement:

I hereby acknowledge that I fail to sign out within 24-hours of signing in or leave the installation without being signed-out; I will be barred from entering any of the installations in the Schweinfurt Community for a period of up to 30 days for the first offense and 60 days for the second consecutive offense and permanently for the 3rd offense..

Einverständniserklärung des Gastes:

Ich erkenne hiermit an, dass mir der Zutritt zu den US Einrichtungen in Schweinfurt Community beim ersten Verstoss fuer bis zu 30 Tage, beim zweiten Verstoss fuer bis zu 60 Tage und beim dritten Verstoss permanent gesperrt werden kann, wenn ich mich nicht innerhalb von 24 Stunden, nachdem ich mich eingeschrieben habe, wieder austrage, oder, wenn ich die Einrichtung verlasse ohne mich auszutragen.

 Guest #1 / Signature Guest #2 / Signature Guest #3 / Signature Guest #4 / Signature
 Gast #1 / Unterschrift Gast #2 / Unterschrift Gast #3 / Unterschrift Gast #4 / Unterschrift

PRIVACY ACT STATEMENT: Authority – Section 6311 of Title 5 to USC authorizes collection of this information. Principal Purpose – To control local access to installations, buildings, and controlled spaces. Routine Uses – The social security number provides an interface with Installation Access Control Systems. Disclosure – Disclosure is voluntary, but failure to provide the requested information may result in denial of access to DOD facilities.

Signed out: Date / Time _____ / _____

Guard's Initials/ badge#: _____ / _____

USAG SCHWEINFURT SUMMARY SHEET
CONTINUATION (PAGE 2)

REMARKS (Con't):