

5 AUGUST 2004



Security

INSTALLATION ACCESS CONTROL SYSTEM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ USAFE/SFOS
(SMSgt Robert L. Sealey)

Certified by: HQ USAFE/SFOS
(Maj Robert S. Kafka)

Pages: 33
Distribution: F

This Instruction implements Air Force Policy Directive 31-2, *Law Enforcement*. It prescribes policy and procedures for utilization of the Installation Access Control System (IACS) to support installation entry control. It outlines enrollment procedures utilized when registering personnel in the IACS and instructions for preparing and issuing the IACS produced United States Army Europe (USAREUR) and United States Air Forces Europe (USAFE) Installation Pass (IP). Procedures outlined in this instruction describe the purpose and applicability of IACS and are used in conjunction with local access control procedures prescribed in each wing's Installation Security Instruction (ISI). It applies to all personnel requiring access to military-controlled installations in USAFE where the IACS is fielded. As other USAFE Installations transition to the IACS, they must comply with this instruction within 4 months of receiving IACS to allow reasonable time to complete enrollment of their base populace. It also applies to Air National Guard or Air Force Reserve units in the USAFE Area of Responsibility (AOR). Installations utilizing the IACS will supplement this instruction or create unit instructions as necessary to meet local requirements according to AFI 33-360V1, *Publications Management Program*. Supplements must be coordinated through the USAFE Security Forces Operations Branch at HQ USAFE/SFOS, Unit 3050, Box 135, APO AE 09094-0135. The Privacy Act, 1974, applies to this regulation. The authority to collect and maintain the information for the Installation Access Control System is Sections 3013, 5013, and 8013, Title 10, United States Code, and Executive Order 9397. System of Records Notice F031 AF SPO "Documentation for Identification and Entry Authority" applies. The rights of individuals under the Privacy Act of 1974, 5 U.S.C. Section 552a, with the exception of subsection (i) regarding criminal penalties will be applied to Local National employees analogously. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at: <https://webrims.amc.af.mil>.

Section A General Information 4

1. Program Overview: 4

2. Responsibilities: 5

3. Exceptions to Policy: 7

Section B Installation Access 7

4. Access Methods: 7

5. DoD ID-Card-Holder Access to Installations: 7

6. USAFE Installation Passes (IPs): 8

Figure 1. Sample USAREUR/USAFE IP. 9

Figure 2. Sample Temporary USAREUR/USAFE IP. 9

Section C Installation Access Control System (IACS) 10

7. IACS Registration: 10

8. DoD ID-Card Holder: 11

9. Local National Employee (LN): 12

10. Contractor (Based in United States): 13

11. Contractor (Living in Host Nation): 14

12. Personal-Service Employee: 15

13. Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract) 16

14. Vendor and Commercial Solicitor: 17

15. NATO Member: 17

16. Foreign Student (Marshall Center): 18

17. Member of Private Organization: 19

18. Visitor (Immediate Family Member Living in Europe): 19

19. Visitor: 19

20. Official Guest: 20

21. Department Of State and American Embassy Personnel: 21

22. Other: 22

Section D Installation Pass 23

23. Application Process: 23

Section E Installation Access Control Office (IACO) 25

24.	General:	25
25.	Registration Procedures for Installation-Pass Applicant:	26
26.	Registration Procedures for DoD ID-Card Holder:	26
Section F	Access Procedures When Utilizing IACS Verification	27
27.	Identification Card and Installation Pass Holders:	27
28.	Sign-In Procedures:	28
29.	Access Rosters:	28
30.	Security of IACS Related Equipment and Supplies:	29
Section G	Integration and Transition and Adopted Forms	29
31.	Integration of IACS Into Antiterrorism and Force Protection Plans:	29
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		31

Section A—General Information

1. Program Overview:

1.1. Concept of IACS:

1.1.1. The Installation Access Control System (IACS) enhances installation access control by providing an additional layer of security above the traditional method of manual credential check verification. Through the use of technology, identification (ID) credentials may now be electronically validated at installation entry control points. Another advantage of IACS is standardization of access documents throughout USAFE for non-DoD ID card holders. Once fielding of the system is complete, the IACS-produced pass will be accepted at all military installations and facilities in the European Theater of Operations, regardless of where the access document was issued. This does not include situations in which entry controllers have reason to question the authenticity of the access document.

1.2. Integration of IACS:

1.2.1. The integration of IACS into daily installation access control procedures aids the prevention of unauthorized access to the installation by providing the capability to:

1.2.2. Detect attempts to access installations using forged, invalid, or unauthorized access documents.

1.2.3. Query a database of information on individual access privileges that is networked to military installations throughout Germany and eventually the entire European theater.

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

1.2.5. Produce uniquely coded IPs, which may be invalidated by the appropriate approval authorities for cause. IACS produced passes were developed to provide all information necessary to verify an individual's authority to enter the installation during periods when the IACS is not fully operational and manual ID checks become necessary.

1.2.6. Scan bar-coded Department of Defense identification (DoD ID) cards and IACS produced IPs to verify access authorization and privileges.

1.2.7. Maintain an automated historical record of personnel who have accessed USAFE installations.

1.2.8. Receive immediate notification when a barred individual attempts to enter the installation.

1.2.9. Support Force Protection Condition (FPCON) measures related to installation access control.

1.3. Success of IACS:

1.3.1. Sponsoring organizations, approving officials and their responsibilities are critical to the success of Installation Access Control and the overall effectiveness of IACS.

1.4. Individual Access Privileges:

1.4.1. Individual access privileges are risk-based and depend on an individual's "Person Category" as outlined in paragraph 7.4.

2. Responsibilities:

2.1. The Directorate of Security Forces (HQ USAFE/SF):

- 2.1.1. Serves as liaison between USAFE and USAREUR for any IACS-related issues.
- 2.1.2. Provides staff supervision and guidance for utilization of the IACS.
- 2.1.3. Serves as the proponent for USAFE IACS implementation, to include system fielding, testing, life-cycle replacement management, and operator training.
- 2.1.4. Conducts staff assistance visits to review IACS registration and IP issuing procedures.
- 2.1.5. Ensures all installation access control offices (IACO) comply with regulatory requirements outlined in this instruction.
- 2.1.6. Provides oversight for the procurement and security of IP cardstock.

2.2. Installation Commanders:

2.2.1. Ensure the following are incorporated into the Wing ISI:

- 2.2.1.1. Procedures for DoD ID-card holders to register in and withdraw from the IACS during in- and out-processing, respectively, at their servicing IACO. Consider including IACS registration and deregistration on inprocessing and outprocessing checklists. Since IACS is designed to associate each DoD ID with a specific individual, reregistration is required anytime an ID card is reissued for any reason (i.e. loss, confiscation or normal replacement).
- 2.2.1.2. Procedures for retrieving IPs from individuals who no longer require installation access.
- 2.2.1.3. Provisions to ensure only users who have been trained to operate the IACS have access to the IACS equipment.
- 2.2.1.4. Security of IACS equipment against theft or damage at IACOs and access control points. If the facility where the equipment is housed cannot be secured, the equipment must be removed at the end of the duty day.

2.3. **Security Forces Administration Sections.** Ensure current barment information is provided to HQ USAFE/SFOS on a monthly basis for addition to the IACS master database.

2.4. **Contracting Offices.** Include a contract provision to ensure that contractors return all IPs to the issuing IACO when the contract is completed or when a contractor employee no longer requires access to the installation (e.g. quits, is terminated).

2.5. Sponsoring organizations:

2.5.1. Each sponsoring organization will ensure:

- 2.5.1.1. A USAFE Form 79, **Request for Base Entry Identification**, is prepared for each installation-pass applicant.
- 2.5.1.2. The applicant registers his or her vehicle according to the procedures in this instruction and USAFEI 31-202, *Registering and Operating Privately Owned Motor Vehicles in Germany*. Vehicle registration is required for all installation-pass applicants who use a vehicle to enter USAFE installations. Up to three vehicles may be registered for each IP holder.

2.5.1.3. Issued IPs are retrieved and returned to the issuing IACO when the relationship that served as the justification for the IP changes or is terminated.

2.5.1.4. Personnel designated authority to serve as approving officials are identified to the servicing IACO according to the requirements outlined in paragraphs 23.1.2. through 23.1.2.3.

2.6. All personnel:

2.6.1. All personnel requiring recurring and unescorted access to USAFE installations must:

2.6.1.1. Enroll in the IACS and provide digitized fingerprint minutia data (DFMD). This may be obtained during inprocessing or initial pass issue. Fingerprint-data policy is as follows:

2.6.1.1.1. Inprocessing. Personnel who possess an authorized DoD ID card and installation-pass applicants will provide DFMD during the IACS registration process. If a DoD ID-card holder has a manually-produced DoD ID card, the individual must obtain a machine-produced bar-coded DoD ID card according to the appropriate military regulations and personnel systems.

2.6.1.1.2. Identification Verification. Security or appropriate command personnel may require an individual to provide his or her DFMD for identification-verification purposes. This verification may routinely occur at access control points to USAFE installations. When the request for the DFMD extends beyond identifying an individual, "probable cause" or other legal basis must be present before any apprehension or search. If the request for the DFMD leads to an apprehension or search, coordination with a representative of the servicing judge advocate office should occur, if practical. If the apprehension or search involves a host-nation citizen, coordination with the host-nation police will occur. Refusal to provide a DFMD may be the basis for immediate surrender of the individual's IP or DoD ID card and grounds for further administrative or punitive action by the command.

2.6.1.2. Carry their DoD ID card or IP (for non-DoD card holders) on their person while in duty status or when on a USAFE installation. On request, they will present their DoD ID card or IP to military law-enforcement personnel or guards. Individuals who refuse to present their DoD ID card or IP are subject to immediate surrender of the card or pass and may be grounds for further administrative or punitive action.

2.6.1.3. Immediately report a lost or stolen DoD ID card or IP to the local Security Forces (SF) or servicing IACO so the card can be deregistered.

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

2.6.1.5. Turn in the IP to the servicing IACO or sponsoring organization when the pass expires or when the basis for obtaining the IP no longer exists.

2.6.1.6. When planning to use a privately owned vehicle (POV) to enter USAFE installations, non-DoD ID card holders must register his or her POV as part of the IP application process, according to this instruction.

2.7. IACOs. Responsibilities are listed in paragraph 24.

2.8. **IACS Registration Offices.** Upon notification of a lost or stolen DoD ID card or IP, IACS registration offices will immediately flag the record in the IACS to deregister the lost card or pass.

3. Exceptions to Policy:

3.1. Exceptions to policy for enrollment in the IACS may be granted by the Wing Commander or designee, or outlined in the Wing Installation Security Instruction (ISI). However, exceptions may not be recognized at other installations within Germany. Exceptions to policy for USAREUR controlled facilities must be addressed to HQ USAREUR/OPM.

Section B—Installation Access

4. Access Methods:

4.1. Normal Operations:

4.1.1. When utilizing the IACS to support installation access control, entry to USAFE installations is restricted to one of the following four methods:

4.1.2. Have a valid DoD ID card and be registered in the IACS, unless an exception to policy has been granted.

4.1.3. Have a USAREUR/USAFE IP (**Figure 1.** or **Figure 2.**).

4.1.4. Be vouched on base by an authorized individual with sign-in privileges.

4.1.5. Be on an approved access roster.

4.2. Other Considerations for Access or Special Events:

4.2.1. Although IACS is designed to ensure 100 percent accountability of personnel accessing USAFE installations, there may be situations when the use of IACS is not feasible or appropriate (for example, community appreciation events, military convoys, high stressed traffic periods). Each USAFE wing will determine the specific utilization of IACS required to meet their operational needs.

4.2.2. Allowing memorandums, travel orders, Privilege and Identification Cards, passports and other like media to serve as authorized installation access documents defeat the purpose of having the IACS, since the two main benefits of IACS, authorization and accountability, are circumvented. Therefore, all North Atlantic Treaty Organization (NATO) sending states and non-DoD ID card holders requiring routine access to the installations must be required to obtain an IACS issued IP.

5. DoD ID-Card-Holder Access to Installations:

5.1. Perimeters for Access:

5.1.1. When utilizing the IACS, the DoD ID card must have a readable barcode and the DoD ID cardholder must have previously registered in the IACS in order for the system to properly verify the person's access authority.

5.2. Valid DoD ID Card Types:

5.2.1. Once IACS registration is complete, the following machine-produced DoD ID cards are considered valid access documents:

5.2.1.1. DD Form 2S(ACT), **Armed Forces of the United States Geneva Conventions Identification Card** (Active) (Green). This card is issued to active duty military personnel.

5.2.1.2. DD Form 2S(RET), **United States Uniformed Services Identification Card** (Retired) (Blue). This card is issued to military retirees.

5.2.1.3. DD Form 2S(RES), **Armed Forces of the United States Geneva Conventions Identification Card** (Reserve) (Green). This card is issued to Reserve or National Guard personnel.

5.2.1.4. DD Form 2S(RESRET), **Armed Forces of the United States Geneva Conventions Identification Card** (Reserve Retired) (Red). This card is issued to Reserve or National Guard personnel.

5.2.1.5. DD Form 1173, **Uniformed Services Identification and Privilege Card**. This card is issued to eligible military DoD civilian-employee family members.

5.2.1.6. DD Form 1173-1, **Department of Defense Guard and Reserve Family Member Identification Card** (Tan). This card is issued to eligible military DoD civilian-employee family members.

5.2.1.7. DD Form 2764S, **United States Department of Defense/Uniformed Services Civilian Geneva Conventions Identification Card** (Tan). This card is issued to emergency-essential civilians and civilian-contract employees.

5.2.1.8. DD Form 2765S, **Department of Defense/Uniformed Services Identification and Privilege Card** (Tan). This card is issued to General Schedule employees and DoD contractors with logistical support.

5.2.1.9. Common Access Card (CAC), **Armed Forces of the United States Identification Card**. CACs with a green stripe are issued to DoD contractors who are authorized individual logistical support and processed as DoD ID-card holders for the purpose of IACS registration. **EXCEPTION:** CACs with a red vertical stripe on the right side of the card are not recognized by USAREUR and USAFE entry controllers as an authorized access document. Personnel possessing a red-striped CAC will require issue of an IP if base access is required. **NOTE:** The USAFE Form 174, **USAFE Privilege and Identification Card**, and AE Form 600-700A, **USAREUR Privilege and Identification Card**, will continue to be a valid access document until the IACS is operational. Once the IACS is activated throughout Germany, these forms will no longer be valid as a means of installation entry. However, the forms remain valid as a privilege card and therefore should not be confiscated unless their use was fraudulent.

6. USAFE Installation Passes (IPs):

6.1. Recognized Types of IPs:

6.1.1. The two types of IPs recognized by IACS are the USAREUR/USAFE IP and the Temporary USAREUR/USAFE IP, which henceforth are referred to as the IP and Temporary IP, respectively.

6.2. Descriptions and Examples of IPs:

6.2.1. Temporary IPs have a red background in the title block to distinguish them from the IP, which has a green background. **Figure 1.** and **Figure 2.** show samples of both passes. Although these IPs are standardized in appearance, the restrictions associated with each pass are different depending on the recipient’s access requirements. **NOTE:** Once fielding of the IACS is complete, the USAFE Form 77, **Base Entry Identification**, will no longer be issued by agencies in Germany. However, USAFE Form 77 will still be used by other bases throughout USAFE until complete integration to IACS. Holders of USAFE Form 77 issued outside of Germany, but performing temporary duty (TDY) in Germany, must register in IACS and receive a temporary IP for the duration of their TDY. **Do not confiscate their USAFE Form 77.**

Figure 1. Sample USAREUR/USAFE IP.



Figure 2. Sample Temporary USAREUR/USAFE IP.



6.3. Non-valid USAREUR Forms:

6.3.1. Upon implementation of IACS, the following USAREUR forms are no longer valid: all editions of the 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**.

6.4. IACOs will not alter IPs:

6.4.1. IACOs will not alter the appearance of IPs with Installation-unique features (for example, custom stamps, stickers, holograms).

6.5. Differences between Temporary IPs and IPs:

6.5.1. The differences between the Temporary IP and IP include:

6.5.2. A Temporary IP is valid for up to 90 days.

6.5.3. If an IP is desired, a Temporary IP may be issued pending completion of a required background check as it will be outlined in USAFEI 31-501, *Local National Background Investigations In Germany*, and local policy. This balances security concerns with operational requirements. The use of successive Temporary IPs is discouraged, but may be warranted to meet operational needs. Wing Commanders will determine circumstances and duration for extension of a Temporary IP.

6.6. Application procedures for IACS:

6.6.1. Application procedures outlined in paragraph 23. must be completed before IACS registration may begin.

Section C—Installation Access Control System (IACS)

7. IACS Registration:

7.1. USAFE Installations:

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

7.2. Self-Registration:

7.2.1. The IACS is designed to record access to the installation by nonregistered DoD ID-card holders through a self-registration option. This option ensures 100 percent accountability of all personnel who have entered the installation and, if used, will cause nonregistered DoD ID-card holders a minor delay each time they enter an installation. The intent is to encourage nonregistered personnel to enroll in the IACS. Excessive entry (15 occurrences) by nonregistered personnel will result in the individual being flagged at Office of the Provost Marshall (OPM). Although the individual will not be denied entry, OPM will contact the IACO to determine why the individual has not been enrolled in the IACS. The underlying purpose of flagging records is to help identify possible unauthorized DoD ID-card holders.

7.3. Application Procedures for IPs:

7.3.1. Application procedures for IPs are provided in paragraph 23.

7.4. Individual Categories for Registration:

7.4.1. Under the IACS, an individual must be registered in one of the following person categories:

7.4.2. DoD ID-Card Holder.

7.4.3. Local National Employee (LN).

7.4.4. Contractor (Based in United States).

7.4.5. Contractor (Living in Host Nation).

7.4.6. Personal-Service Employee.

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

7.4.8. Vendor or Commercial Solicitor.

7.4.9. NATO Member.

7.4.10. Foreign Student (Marshall Center).

7.4.11. Member of Private Organization.

7.4.12. Visitor (Immediate Family Member Living in USAFE).

7.4.13. Visitor (Friend or Family Member Not Included in Category Above).

7.4.14. Official Guest.

7.4.15. Department of State and U.S. Embassy Personnel.

7.4.16. Other.

7.5. Dual-Category Individuals:

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

7.6. Access Restrictions:

7.6.1. Each category is risk-based. Specific requirements for registration and access restrictions for each category are in paragraphs 8. through 23.

8. DoD ID-Card Holder:

8.1. Term Definition.

8.1.1. An individual authorized to possess a DoD ID card, to include children 10 years and older. The status of a DoD ID-card holder will supersede other person categories. For example, an LN employee, married to a service member and entitled to a DD Form 1173, **Uniformed Services Identification and Privilege Card**, will be treated as a DoD ID-card holder for the purpose of this regulation and will not be issued an IP nor require sponsoring.

8.2. Type of Pass Authorized:

8.2.1. Not applicable. 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 during community inprocessing to be registered in the IACS, but will not be issued an IP. Individuals who have multiple DoD ID cards (for example, a military retiree who is now a DoD civilian employee) must use the DoD ID card used for IACS registration to access the installation, however, they will not be required to surrender their other ID card.

8.3. Length of Time Registration is Valid:

8.3.1. For personnel with an established date eligible for return from overseas (DEROS), registration is valid 15 days past their DEROS or 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 USAFE

temporarily, 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 to visit their servicing IACO to update the expiration date of the IACS registration.

8.4. Sponsor Requirements:

8.4.1. DoD ID-card holders may self-sponsor and do not need to provide documentation beyond their previously issued ID when enrolling in IACS. Minors will be registered in the presence of a parent or legal guardian.

8.5. Background Checks:

8.5.1. Not applicable

8.6. Resident and Work Permits:

8.6.1. Not applicable.

8.7. Restrictions on Number of Installations a DoD ID-Card Holder May Enter:

8.7.1. No restrictions apply, unless imposed by an authorized commander.

8.8. Restrictions on Days and Times Access is Authorized:

8.8.1. No restrictions apply, unless imposed by an authorized commander.

8.9. Restrictions on Sign-In Privileges:

8.9.1. Restrictions are determined by the Host Installation Commander and identified in the Installation Security Instruction.

8.10. FPCON Restrictions:

8.10.1. No restrictions apply.

9. Local National Employee (LN):

9.1. Term Definition:

9.1.1. An individual who is employed by or performing duties in support of the DoD in USAFE, but is not entitled to unrestricted access to DoD Installations. This person category is primarily for host-nation employees in USAFE.

9.2. Type of Pass Authorized:

9.2.1. Temporary IP. Authorized to allow access while background checks are being conducted.

9.2.2. IP. Authorized after all background checks have been completed.

9.3. Length of Time Pass is Valid:

9.3.1. A Temporary IP is valid for up to 90 days. An IP is valid for up to 5 years or the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

9.4. Sponsor Requirements:

9.4.1. The Civilian Personnel Office or the organization that the Local National (LN) employee will work for will perform the sponsor responsibilities in this instruction.

9.5. Background Checks:

9.5.1. Background checks will be conducted in accordance with AFI 31-501, *Personnel Security Program Management*, and local policy.

9.6. Resident and Work Permits:

9.6.1. These permits may be required if the applicant is not a host-nation or European Union (EU) resident.

9.7. Restrictions on the Number of Installations a Pass Holder May Enter:

9.7.1. 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.

9.8. Restrictions on Days and Times Access is Authorized:

9.8.1. No restrictions apply unless specified by the sponsor.

9.9. Restrictions on Sign-In Privileges:

9.9.1. Temporary Pass holders are not authorized sign-in privileges. IP holders are not authorized sign-in privileges unless justified by the sponsoring organization in writing. If sign-in privileges are justified, the IP holder may sign-in up to four individuals and their vehicles "for official business only." (Does not apply to special categorized employees outlined in USAFEI 36-725, *USAFE Civilian Service Program (Germany)*). Sign-in privileges for IP holders are not authorized during FPCON Delta. Wings may grant exceptions to this restriction for their Installation only. Exceptions will be entered in the REMARKS section on the back of the IP.

9.10. FPCON Restrictions:

9.10.1. As determined locally.

10. Contractor (Based in United States):

10.1. Term Definition:

10.1.1. A contractor who lives in the United States and is contracted to work for DoD in the USAFE AOR, but is not a DoD ID-card holder. Although this individual is authorized an IP, the pass is specially designed for contractors from the United States, but working in USAFE temporarily under official government travel orders.

10.2. Type of Pass Authorized:

10.2.1. Temporary IP: Authorized.

10.2.2. IP: Authorized if in the USAFE AOR longer than 90 consecutive days.

10.3. Length of Time Pass is Valid:

10.3.1. The Temporary IP is valid for the length of the visit or up to 90 days, whichever is earlier. The IP is valid for the length of visit (must be more than 90 consecutive days), for up to 1 year, or at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

10.4. Sponsor Requirements:

10.4.1. The organization inviting the contractor to or escorting the contractor in USAFE will perform the sponsor responsibilities in this instruction.

10.5. Background Checks:

10.5.1. Not applicable.

10.6. Resident and Work Permits:

10.6.1. A resident permit may be required.

10.7. Restrictions on Number of Installations a Pass Holder May Enter:

10.7.1. The number of installations will be limited to the minimum required for the contractor to perform his or her duties.

10.8. Restrictions on Days and Times Access Authorized:

10.8.1. No restrictions apply unless specified by the sponsor.

10.9. Restrictions on Sign-In Privileges:

10.9.1. Not authorized.

10.10. FPCON Restrictions:

10.10.1. As determined by the contract or local wing FPCONs.

11. Contractor (Living in Host Nation):**11.1. Term Definition:**

11.1.1. A contractor who lives in the host nation, is contracted to work for DoD in the USAFE AOR, and is not a DoD ID-card holder.

11.2. Type of Pass Authorized:

11.2.1. Temporary IP: Authorized to allow access while background checks are being conducted.

11.2.2. IP: Authorized after all background checks have been completed.

11.3. Length of Time Pass is Valid:

11.3.1. A Temporary IP is valid for the length of the contract or up to 90 days, whichever is earlier. The IP is valid for the length of the contract, up to 2 years, or at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

11.4. Sponsor Requirements.

11.4.1. The organization hiring the contractor will perform the sponsor responsibilities in this instruction.

11.5. Background Checks:

11.5.1. Background checks will be conducted in accordance with AFI 31-501 and local policy.

11.6. Resident and Work Permits:

11.6.1. These permits may be required for non-German citizens, unless the non-German citizen is an exception to this requirement.

11.7. Restrictions on Number of Installations Pass Holder May Enter:

11.7.1. The number of installations will be limited to the minimum required for the contractor to perform his or her duties.

11.8. Restrictions on Days and Times Access Authorized:

11.8.1. No restrictions apply unless specified by the sponsor.

11.9. Restrictions on Sign-In Privileges:

11.9.1. 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 approving official deems it is necessary in the performance of the contract based on the scope of work. For example, construction of a new building would normally justify the prime contractor to have sign-in privileges. Sign-in privileges are only allowed during FPCON Alpha and FPCON Bravo and are limited to signing-in four people and their vehicles. Only other contractors and vendors in support of the contract will be signed in. Sign-in privileges are not authorized for Temporary IP holders.

11.10. FPCON Restrictions.

11.10.1. As determined in the contract or local Wing FPCONs.

12. Personal-Service Employee:

12.1. Term Definition:

12.1.1. A personal-service employee is an individual hired by an individual residing on-base to perform a service (e.g., nanny, dog-sitter, house-cleaner).

12.2. Type of Pass Authorized:

12.2.1. Temporary IP: May be authorized for up to 90 days based on local policy.

12.2.2. IP: Authorized after all background checks have been completed.

12.3. Length of Time the Pass is Valid:

12.3.1. The Temporary IP is valid for the length of service or up to 90 days, whichever is earlier. The IP is valid for the length of service, for 2 years, or at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

12.4. Sponsor Requirements:

12.4.1. The Host Installation commander will determine requirements and list them in the Installation Security Instruction.

12.5. Background Checks:

12.5.1. Background checks will be conducted in accordance local policy.

12.6. Resident and Work Permits:

12.6.1. These permits may be required for non-German citizens.

12.7. Restrictions on Number of Installations a Pass Holder May Enter:

12.7.1. Access will be limited to one installation, either to where the sponsor is employed, or where they reside.

12.8. Restrictions on Days and Times Access is Authorized:

12.8.1. No restrictions apply unless specified by the requester, sponsor or approving official.

12.9. Restrictions on Sign-In Privileges:

12.9.1. Not authorized.

12.10. FPCON Restrictions:

12.10.1. Determined locally.

13. Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract)**13.1. Term Definition:**

13.1.1. Delivery personnel are individuals who need recurring access to USAFE installations to make deliveries or perform a similar service that is related to their employment (for example, pizza delivery, taxi driver).

13.2. Type of Pass Authorized:

13.2.1. Temporary IP: Not authorized.

13.2.2. IP: Authorized after all background checks have been completed.

13.3. Length of Time Pass is Valid:

13.3.1. The IP is valid for up to 2 years or expires on the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

13.4. Sponsor Requirements:

13.4.1. Determined by the Host Installation and outlined in the Installation Security Instruction.

13.5. Background Checks.

13.5.1. Background checks will be conducted in accordance with local policy.

13.6. Resident and Work Permits:

13.6.1. Required for non-German citizens.

13.7. Restrictions on Number of Installations a Pass Holder May Enter:

13.7.1. Not to exceed the sponsoring Installation.

13.8. Restrictions on Days and Times Access Authorized:

13.8.1. As determined by the sponsor.

13.9. Restrictions on Sign-In Privileges:

13.9.1. Not authorized.

13.10. FPCON Restrictions:

13.10.1. IPs for delivery personnel are valid only at FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host Wing.

14. Vendor and Commercial Solicitor:**14.1. Term Definition:**

14.1.1. Vendors and commercial solicitors are individuals who are authorized to sell merchandise or provide services on USAFE installations.

14.2. Type of Pass Authorized:

14.2.1. Temporary IP: Not authorized.

14.2.2. IP: Authorized after all background checks have been completed.

14.3. Length of Time Pass is Valid:

14.3.1. The IP is valid for up to 2 years, or expiration date of the supporting document (for example, passport) that was used to obtain the IP, or at the expiration date of the commercial solicitation or vendor permit.

14.4. Sponsor Requirements:

14.4.1. Determined by the Host Installation.

14.5. Background Checks:

14.5.1. Background checks will be conducted in accordance with local policy.

14.6. Resident and Work Permits:

14.6.1. Required for non-German citizens, unless the non-German citizen is an exception to this requirement.

14.7. Restrictions on Number of Installations a Pass Holder May Enter:

14.7.1. Not to exceed the sponsoring Installation.

14.8. Restrictions on Days and Times Access Authorized:

14.8.1. No restrictions apply unless specified by the sponsor.

14.9. Restrictions on Sign-In Privileges:

14.9.1. Not authorized.

14.10. FPCON Restrictions:

14.10.1. Valid during FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host wing.

15. NATO Member:**15.1. Term Definition:**

15.1.1. NATO members are NATO military personnel, civilian employees, and their family members who reside in or require routine access to installations in Germany.

15.2. Type of Pass Authorized.

15.2.1. Temporary IP: Not applicable.

15.2.2. IP: Authorized.

15.3. Length of Time Pass is Valid:

15.3.1. The IP for a NATO member is valid for up to 5 years, for the length of the member's tour, or at the expiration date of the supporting document (for example, a military ID card) that was used to obtain the IP, whichever is earlier.

15.4. Sponsor Requirements:

15.4.1. Sponsor requirements apply to the following subcategories:

15.4.1.1. NATO Members assigned to an International Military Headquarters, Activity, or Special Mission in USAFE. The parent organization will be the sponsor for this person category and will perform the sponsor responsibilities in this instruction. Sponsor requirements will be determined locally.

15.4.1.2. Active-Duty Belgium, British, Canadian, Dutch, and French Military Stationed in Germany (also known as Sending States). Sponsor requirements will be determined locally.

15.4.1.3. French and British Consular and Diplomatic Personnel Stationed in Germany. Sponsor requirements will be determined locally.

15.5. Background Checks:

15.5.1. Not required.

15.6. Resident and Work Permits:

15.6.1. Not required.

15.7. Restrictions on Number of Installations a Pass Holder May Enter:

15.7.1. No restrictions. NATO members are automatically granted access to USAFE installations and facilities. No justification is required.

15.8. Restrictions on Days and Times Access Authorized:

15.8.1. No restrictions.

15.9. Restrictions on Sign-In Privileges:

15.9.1. Limited to signing-in four persons and their vehicles.

15.10. FPCON Restrictions:

15.10.1. No restrictions.

16. Foreign Student (Marshall Center):**16.1. Term Definition:**

16.1.1. Foreign military students assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany. USAREUR is the action office for enrollment of these person-

nel. These personnel have limited access to Advanced Security Training (AST) facilities in Garmisch and are not granted unescorted access to USAFE installations.

17. Member of Private Organization:

17.1. Term Definition:

17.1.1. A member of an approved private organization who has no other reason to enter USAFE installations other than to participate in private organization functions.

17.2. Type of Pass Authorized:

17.2.1. Temporary IP: Not authorized.

17.2.2. IP: Authorized per local directives.

17.3. Length of Time Pass is Valid:

17.3.1. The IP is valid for up to 2 years or at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

17.4. Sponsor Requirements:

17.4.1. The Installation where the private organization function takes place will perform the sponsor responsibilities in this regulation.

17.5. Background Checks:

17.5.1. Background checks will be conducted in accordance with local policy.

17.6. Resident and Work Permits:

17.6.1. Not applicable.

17.7. Restrictions on Number of Installations a Pass Holder May Enter:

17.7.1. Not to exceed the individual's sponsoring Installation. The sponsoring Installation may also impose further restrictions.

17.8. Restrictions on Days and Times Access Authorized:

17.8.1. No restrictions unless imposed by the sponsoring Installation.

17.9. Restrictions on Sign-In Privileges:

17.9.1. Not authorized.

17.10. FPCON Restrictions:

17.10.1. Valid during FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host Wing.

18. Visitor (Immediate Family Member Living in Europe):

18.1. This category is exclusive to USAREUR personnel and will not be utilized by USAFE for installation access control. USAFE Installations will register non-DoD family members and visitors according to paragraph [19](#). below.

19. Visitor:

19.1. Term Definition.

19.1.1. A visiting family member or friend of the requester who is not authorized a DoD Identification Card.

19.2. Type of Pass Authorized.

19.2.1. Temporary IP: Authorized.

19.2.2. IP: Not authorized.

19.3. Length of Time Pass is Valid:

19.3.1. The Temporary Pass is valid for the length of the visit or up to 90 days, whichever is earlier. **NOTE:** Visits beyond 90 days will require a renewal Temporary IP be issued. Applicants must register with the Foreign Affairs Office and obtain an extended visitor/tourist visa prior to Temporary IP renewal.

19.4. Sponsor Requirements:

19.4.1. The requester will be the sponsor for this person category and will perform the sponsor responsibilities in this regulation.

19.5. Background Checks:

19.5.1. Not required.

19.6. Resident and Work Permits:

19.6.1. Not applicable.

19.7. Restrictions on Number of Installations a Pass Holder May Enter:

19.7.1. Not to exceed the immediate community of the requestor.

19.8. Restrictions on Days and Times Access Authorized:

19.8.1. No restrictions unless imposed by the requester or sponsor.

19.9. Restrictions on Sign-In Privileges:

19.9.1. Not authorized.

19.10. FPCON Restrictions:

19.10.1. IPs are only valid during FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host Wing.

20. Official Guest:**20.1. Term Definition:**

20.1.1. 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 person category when the applicant meets the definition of another, more restrictive person category. This category is specifically designed for personnel, who by their position or

standing within the community, are considered trustworthy. Local policy will determine who may be issued Official Guest passes.

20.2. Type of Pass Authorized:

20.2.1. Temporary IP: Authorized.

20.2.2. IP: Authorized.

20.3. Length of Time Pass is Valid:

20.3.1. A Temporary IP is valid for up to 90 days. An IP is valid for up to 2 years or at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

20.4. Sponsor Requirements:

20.4.1. The organization escorting the guest will be the sponsor for this person category and will perform the sponsor responsibilities in this regulation.

20.5. Background Checks:

20.5.1. Determined locally.

20.6. Resident and Work Permits:

20.6.1. Not required.

20.7. Restrictions on Number of Installations a Pass Holder May Enter:

20.7.1. The number of installations will be limited to the minimum required for the guest to conduct official business.

20.8. Restrictions on Days and Times Access Authorized:

20.8.1. Specified by the sponsoring organization.

20.9. Restrictions on Sign-In Privileges:

20.9.1. Not authorized, unless justified by the sponsoring organization. If authorized, sign-in privileges are limited to signing-in four individuals and their vehicles only for official business.

20.10. PCON Restrictions:

20.10.1. IPs are only valid during FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host Wing.

21. Department Of State and American Embassy Personnel:

21.1. Term Definition:

21.1.1. An individual assigned to or on duty with the United States Department of State, an American Embassy in the United States European Command, or in U.S. diplomatic or consular posts.

21.2. Type of Pass Authorized.

21.2.1. Temporary IP: Not authorized.

21.2.2. IP: Authorized.

21.3. Length of Time Pass is Valid:

21.3.1. The IP is valid for the length of the tour, not to exceed 5 years or the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

21.4. Sponsor Requirements:

21.4.1. The United States Mission, Germany (Department of State) is the sponsor for this person category and performs the sponsor responsibilities in this instruction. Wing instructions will outline prerequisites for Embassy personnel to receive an Installation Pass. Normally, a memorandum from the United States Mission, Germany (Department of State) is sufficient documentation.

21.5. Background Checks:

21.5.1. Not required.

21.6. Resident and Work Permits:

21.6.1. Not required.

21.7. Restrictions on Number of Installations a Pass Holder May Enter:

21.7.1. No restrictions.

21.8. Restrictions on Days and Times Access Authorized:

21.8.1. None.

21.9. Restrictions on Sign-In Privileges:

21.9.1. Limited to signing-in four persons and their vehicles.

21.10. FPCON Restrictions:

21.10.1. None.

22. Other:**22.1. Term Definition:**

22.1.1. An individual who requires recurring and unescorted access, but does not meet the definition of another person category. Sponsoring organizations will not use this person category if the applicant meets the definition of another, more restrictive person category. This category is appropriate for a former spouse without base privileges whose children are military dependents with base privileges, but are not old enough to utilize base facilities without parental supervision.

22.2. Type of Pass Authorized:

22.2.1. Temporary IP: Authorized.

22.2.2. IP: Authorized.

22.3. Length of Time Pass is Valid:

22.3.1. A Temporary IP is valid for up to 90 days. An IP will not exceed one year or expire at the expiration date of the supporting document (for example, passport) that was used to obtain the IP, whichever is earlier.

22.4. Sponsor Requirements:

22.4.1. Sponsor requirements are determined locally.

22.5. Background Checks:

22.5.1. Determined locally.

22.6. Resident and Work Permits:

22.6.1. Not required.

22.7. Restrictions on Number of Installations a Pass Holder May Enter:

22.7.1. Not to exceed the sponsoring installation. The sponsoring installation may also impose further restrictions.

22.8. Restrictions on Days and Times Access Authorized:

22.8.1. Determined by the sponsoring organization.

22.9. Restrictions on Sign-In Privileges:

22.9.1. Not authorized.

22.10. FPCON Restrictions:

22.10.1. IPs are only valid during FPCON Alpha and FPCON Bravo. Additional restrictions may be imposed by the host Wing.

Section D—Installation Pass

23. Application Process:

23.1. Using the USAFE FORM 79:

23.1.1. Applications for an IP may be made for the following reasons and will be made using the USAFE Form 79.

23.1.1.1. Reason for Issue. An individual may apply for an IP for one of the following reasons:

23.1.1.2. Initial issue.

23.1.1.3. To obtain an IP after the applicant has received a Temporary IP.

23.1.1.4. Renewal.

23.1.1.5. The original IP was lost or stolen.

23.1.1.6. To extend a Temporary IP.

23.1.1.7. Replace an unserviceable IP.

23.1.2. Approving Official.

23.1.2.1. The approving official is key to the integrity of the USAFE Installation Access Control Program.

23.1.2.2. Unit commanders will designate approving officials in writing. If the sponsoring organization does not have a military rank or civilian pay grade structure (for example, Army and Air Force Exchange Service (AAFES), military banking facilities, government travel

agency and activities), the local senior manager or deputy of the organization is authorized to sign the USAFE Form 79.

23.1.2.2.1. Approving officials must have a DD Form 577, **Appointment/Termination Record--Authorized Signature**, or a signature memorandum on file with IP pass issuing officials prior to signing USAFE Form 79.

23.1.2.3. NATO Sending States and the United States Mission, Germany, will submit their approving official designation memorandum to the appropriate Wing agency that will validate the document and provide it to the IACO.

23.1.2.4. Approving officials will ensure the requirements and intent of this regulation are followed.

23.1.3. Person Category. An applicant's person category governs the type of IP issued and the associated restrictions. Approving officials will state the person category on the USAFE Form 79. IACO issuing officials will verify its correctness. The registration requirements and restrictions vary among person categories, based on risk.

23.1.4. Type of IP Requested. Sponsors will request either the Temporary IP or IP based on the applicant's person category and the circumstances under which the applicant is applying.

23.1.5. Background Checks. Background checks are conducted to determine if an IP applicant is a security risk. Background-check requirements are based on an individual's person category. Sponsoring organizations are responsible for completing required background checks. IACO issuing officials will require verification that a background check has been completed or, when applicable, that a background check has been initiated. Sponsoring organizations should reference the appropriate person category to determine the exact background-check requirements for each applicant.

23.1.6. Number of Installations to Which Access is Required.

23.1.6.1. One of the key objectives of the Installation Access Control Program is to limit access to the minimum number of installations, based on individual requirements.

23.1.6.2. The following person categories are automatically granted access to Air Force/Army installations in Europe without being required to provide justification:

23.1.6.2.1. DoD ID-card holder.

23.1.6.2.2. NATO members.

23.1.6.2.3. Department of State and American Embassy Personnel.

23.1.6.3. For all other Person categories, justification is required for an individual to gain access to installations, the individual's approving official will ensure the USAFE Form 79 shows the minimum number of installations to which access is required by listing the specific name of the installation (for example, Ramstein AB, Spangdahlem AB only). If access is required to more than one installation, provide detailed justification.

23.1.6.4. If justification is required for an individual to enter installations in Europe, the IACO issuing official will:

23.1.6.4.1. Ensure the level-of-access requested does not exceed the approving official's authority.

23.1.6.4.2. Clarify inadequate justifications by coordinating with the approving official.

23.1.6.4.3. Scrutinize all applications for individuals under the Contractor (Living in Host Nation) person category to ensure the requested level-of-access conforms to the requirements outlined in paragraphs 11.5. through 11.10.

23.1.7. Days and Times Access is Required. Approving officials will ensure the USAFE Form 79 shows the minimum days and times access is required.

23.1.8. Sign-in Privileges. Approving officials may request sign-in privileges for the applicant only if bona fide justification is available. The only exceptions are the “NATO Member” and “Department of State and American Embassy Personnel” person categories, which receive automatic sign-in privileges. In most cases, sign-in privileges will be limited to contractors and individuals on official business.

23.1.8.1. Sign-in privileges are not authorized for Temporary IP holders.

23.1.8.2. Person categories with authorized sign-in privileges may sign-in no more than four individuals and their vehicles.

23.1.9. FPCON Restrictions. Based on an individual’s person category, the IACS will prohibit access beyond the FPCON associated with the category. If approving officials want to further restrict access at any of the FPCON levels, the USAFE Form 79 must indicate the imposed restriction.

23.2. Exceptions to Restrictions:

23.2.1. Exceptions to Restrictions. IACS provides a “free text” option to allow IACOs to manually input installation unique information that will be displayed in the remarks section on the reverse side of the IP/Temporary IP. The free text option will only be used when a request for exception has been approved by the IACO.

23.2.2. Request for exceptions will be submitted to the IACO in memorandum format, signed by the approving official. Exceptions must be exclusive to the Installation issuing the pass. Appropriate exceptions may be granted for escort limitations, FPCON restrictions, or to explain unique circumstances associated with individual entry (e.g. access during school days only).

23.3. Vehicle Information:

23.3.1. Vehicle Information. All individuals applying for an IP will register the vehicles they use to enter installations in Europe. Up to three vehicles may be registered. The following vehicle information must be annotated on the USAFE Form 79.

23.3.1.1. Vehicle Identification Number (VIN).

23.3.1.2. License-plate number.

23.3.1.3. Make, model, year, body type, and color.

Section E—Installation Access Control Office (IACO)

24. General:

24.1. Who is Authorized to Issue IPs:

24.1.1. Only USAREUR/USAFE-approved IACOs are authorized to issue IPs. A complete list of authorized IACOs is available at the installation access control link on the OPM website at <http://www.hqusareur.army.mil/opm/opmhome.html>.

24.2. Limitations on IPs:

24.2.1. With the exception of certain default settings in the IACS, IACOs have few limitations on the type of IPs they may issue. For example, every IACO is authorized to issue a USAFE/USAREUR-wide IP. This authority is based on the assumption that each IACO will follow the policy, procedures, and intent of installation access control directives and that the OPM will monitor the IACS user activity.

24.3. Authorized IACOs:

24.3.1. Authorized IACOs will be approved before the IACS is operational. Requests for additional IACOs or IACS-registration stations after the IACS becomes operational will be submitted through HQ USAFE/SFOS, Unit 3050 Box 135, APO AE 09094-0135.

25. Registration Procedures for Installation-Pass Applicant:

25.1. Procedures:

25.1.1. Registration procedures are determined locally, but should incorporate the following procedures:

25.1.1.1. Verify that the approving official is authorized to perform approving official duties.

25.1.1.2. Retrieve the USAFE Form 79 and verify the form is properly completed according to local guidance. It is critical to the success of the Installation Access Control Program that issuing officials check the supporting documentation to minimize the potential of high-risk individuals obtaining access to USAFE installations.

25.1.1.3. Register the applicant in the IACS with the information provided in the USAFE Form 79. For restrictions that are subject to the approving official's written justification (for example, sign-in privileges, number of installations authorized), the issuing official will clarify any justification that is insufficient as a quality-control check for the overall system.

25.1.1.4. Before finalizing IACS registration, complete a fingerprint-data and name-comparison search to preclude duplication of individual records in the IACS database. This procedure will prevent individuals from obtaining more than one IP.

26. Registration Procedures for DoD ID-Card Holder:

26.1. Procedures:

26.1.1. To register a DoD ID-card holder, issuing officials will:

26.1.2. Verify the DoD ID-card holder's requirement to be registered in the IACS as determined by local policy.

26.2. Code 39 Barcode:

26.2.1. Scan the barcode-39 (long barcode on the back of all CACs and DoD ID cards) to ensure its readability. Entry controllers will scan this barcode after the IACS is operational. If the

Code-39 barcode is defective and not readable, issuing officials will terminate the registration process and direct the DoD ID-card holder to obtain a new card.

26.3. PDF 417 Barcode:

26.3.1. Scan the PDF-417 barcode (smaller barcode located on the front of the CAC and back of other DoD ID cards) on the DoD ID card to populate the data fields in the IACS.

26.3.2. A card with a defective PDF-417 does not need to be reissued, as it will not prevent the card from being read at entry control points. However, a defective PDF-417 will prevent the ability to automatically populate personal data during IACS enrollment.

26.4. Other Information:

26.4.1. Enter any information that was not activated during the DoD ID-card scan.

26.5. Photograph:

26.5.1. Take a digital photograph.

26.6. Fingerprint:

26.6.1. Obtain a digital fingerprint.

Section F—Access Procedures When Utilizing IACS Verification

27. Identification Card and Installation Pass Holders:

27.1. Personal Data Assistant:

27.1.1. Utilizing the Personal Data Assistant, the entry controllers will scan the barcode on the back of the DoD ID card or IP and compare the information displayed on the Personal Data Assistant against the individual possessing the media. The IACS provides positive verification of access authorization for individuals carrying these access documents, therefore 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.

27.2. Procedures when IP Holder is not Registered in IACS:

27.2.1. If scanning reveals that an IP holder is not registered in the IACS, local procedures will determine whether the individual will be required to enroll at the Visitor Control Center or, upon verification their ID card is valid, be encouraged to complete enrollment at their earliest convenience.

27.3. Procedures when ID Card or IP will not Scan:

27.3.1. If a DoD ID card or IP will not scan properly in the IACS (for example, defective barcode), manually validate the individual via the gate module and instruct them to immediately obtain a new DoD ID card or IP. If manual validation reveals the individual is not enrolled in IACS, refer to paragraph [27.2.](#) (above).

27.4. Procedures for Manual Look-Up or Fingerprint Feature:

27.4.1. If a DoD ID-card holder or IP holder has forgotten his or her card or pass, the IACS manual look-up or fingerprint-scan features may be used to verify authorization to enter the installation. The individual may then be granted access if authorized by local policy.

28. Sign-In Procedures:

28.1. Procedures:

28.1.1. Sign-in procedures will be utilized when access to the installation is required and access rosters or the issue of an IP is impractical or unauthorized.

28.1.2. Sign-In Privileges.

28.1.2.1. If for some reason this privilege has been suspended, it will only be shown 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 sentry will know is by checking the IACS at the entry control point.

28.1.2.2. With the exception of individuals in the “NATO Member” and “Department of State and American Embassy Personnel” person categories, IP holders are not granted sign-in privileges unless the sponsoring organization justifies the need. This action is accomplished during the IACS registration process. Sign-in privileges are indicated on the front of all IPs with any qualifications (for example, “contractors and vendors only”) listed in the remarks block on the back. Temporary IP holders are not authorized sign-in privileges.

28.1.3. Restrictions. Both DoD ID-card holders and IP 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 limitation is prohibited. Groups of 5 or more guests may be signed-in utilizing access roster procedures outlined in paragraph [29.](#), below.

28.1.3.1. Installations may use the free-text option to override the four person restriction for their installation only. For example, if an installation pass holder routinely provides escort to local dignitary groups, their IP may be modified to indicate “Unlimited escort privileges for Ramstein AB” in the remarks section on the back of the IP.

28.1.3.2. Installations are responsible for ensuring that DoD ID-card holders and IP holders verify the departure of guests from the base premises. Installations are also responsible to ensure forfeiture of guest base passes to issuing agency once the individual departs the installation.

28.1.4. FPCON Restrictions. Installations will determine escort restrictions during increased FPCONs.

28.1.5. Identification. To record escort information in IACS

28.1.5.1. Open the sign-in module and scan the DoD ID card or IP 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.

28.1.5.2. Enter the names of the individuals being signed in up to the authorized limits (paragraph [28.1.2.](#)). The IACS will automatically check the bar roster to ensure these individuals are not barred from the installation.

29. Access Rosters:

29.1. Utilization:

29.1.1. Access rosters are utilized in lieu of sign-in procedures and temporary passes when these methods of access are impractical or unauthorized.

29.2. Procedures:

29.2.1. Access rosters will be used for events that are nonrecurring and not regularly scheduled, are generally site-specific, and are coordinated in advance (i.e. birthday party guest lists or vendor access during holiday bazaars).

29.2.2. IACOs may enter approved access roster information into the IACS via the access roster module.

29.2.3. Once entered, the information will be available at all installation access control points equipped with IACS. Hard copies of the access roster may be printed for dissemination as needed.

30. Security of IACS Related Equipment and Supplies: Take the following actions, as applicable, to ensure the security, accountability, and procurement of IP material:

30.1. Plastic Cardstock:

30.1.1. The plain white plastic cardstock does not require any special security or accountability procedures.

30.2. Security Laminate:

30.2.1. Ensure the IP “security laminate” is under lock and key and stored in a cool and dry place when not in use.

30.3. Loss or Theft of Laminate Materials:

30.3.1. Incidents involving loss or theft of security laminate material from an IACO will be investigated promptly by the Security Forces and reported to HQ USAFE/SFOS.

30.4. Destruction of IPs:

30.4.1. IACO issuing officials will record the destruction of any IP in the IACS.

30.5. Supplies:

30.5.1. IACOs will receive IP cardstock and security laminates from the OPM and maintain adequate stock at all times.

Section G—Integration and Transition and Adopted Forms

31. Integration of IACS Into Antiterrorism and Force Protection Plans: The key to integrating the IACS into an effective Installation Access Control Program is to link it to Antiterrorism and Force Protection (AT/FP) plans and the Random Antiterrorism Measures (RAM) Program. Commanders will prescribe policy and procedures for utilization of the IACS in Wing Instructions, Special Security Instructions (SSIs), AT/FP plans, and RAM Program.

31.1. Forms or IMTs Adopted. DD Form 2S(ACT), **Armed Forces of the United States Geneva Conventions Identification Card (Active) (Green)**, DD Form 2S(RET), **United States Uniformed Services Identification Card (Retired) (Blue)**, DD Form 2S(RES), **Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)**, DD Form 2S(RESRET), **Armed Forces of the United States Geneva Conventions Identification Card (Reserve Retired) (Red)**, DD Form 1173, **Uniformed Services Identification and Privilege Card**, DD Form 1173-1, **Department of Defense Guard and Reserve Family Member Identification Card (Tan)**, DD Form

2764S, United States Department of Defense/Uniformed Services Civilian Geneva Conventions Identification Card (Tan), DD Form 2765S, Department of Defense/Uniformed Services Identification and Privilege Card (Tan), USAFE Form 77, Base Entry Identification, USAFE Form 79, Request for Base Entry Identification, USAFE Form 174, USAFE Privilege and Identification Card, AE Form 190-13A, Permanent U.S. Army IP, AE Form 190-13B, Application for Permanent U.S. Army Europe Installation Pass, AE Form 190-13C, Temporary U.S. Army Europe IP, AE Form 600-410C, Civilian Support Identification Card, AE Form 600-700A, USAREUR Privilege and Identification Card.

MATHEW S. TOTH, Colonel, USAF
Director of Security Forces

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 9397

Privacy Act, 1974

10 USC 3013, 5013, 8013

NATO SOFA SA

AFI 10-245, *Air Force Antiterrorism Standards*

AFI 31-101, *The Air Force Installation Security Program*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI33-360V1, *Air Force Content Management Program - Publications*

AFI 36-3026, *Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel*

USAFE Instruction 31-202, *Registering and Operating Privately Owned Motor Vehicles in Germany*

USAFEI 36-725, *USAFE Civilian Service Program (Germany)*

Abbreviations and Acronyms

AAFES-Eur—Army and Air Force Exchange Service, Europe

AOR—area of responsibility

AT/FP—antiterrorism and force protection

CAC—Common Access Card

DEERS—Defense Enrollment Eligibility Reporting System

DEROS—date eligible for return from overseas

DFMD—digitized fingerprint minutia data

EU—European Union

FPCON—force protection condition

IACO—Installation Access Control Office

IACS—Installation Access Control System

ID—identification

IP—Installation Pass

ISI—Installation Security Instruction

MPF—Military Personnel Flight

NAF—nonappropriated fund

NATO—North Atlantic Treaty Organization

OPM—Office of the Provost Marshal, HQ USAREUR/7A

PCS—permanent change of station

RAM—random anti-terrorism measures

SOFA—Status of Forces Agreement

TDY—temporary duty

USAREUR—United States Army Europe

USAFE—United States Air Forces in Europe

VIN—Vehicle Identification Number

Terms

Access Roster—An approved list of individuals authorized unescorted access to an installation.

Applicant—An individual applying for an IP.

Contractor—An individual working under contract for DoD, to include subcontractors (individuals contracted by the primary contractor to perform portions of a contract), primary contractors, and individual contractors.

Controlled Access Installation—Any USAFE/USAREUR installation where access is controlled by guards.

Installation Access Control Office (IACO)—An office formally designated by the Office of the Provost Marshal, HQ USAREUR/7A, to register individuals into the Installation Access Control System and authorized to produce and issue IPs.

Installation Access Control System (IACS)—The personnel access verification system designed to enhance Installation Entry Control through the utilization of a database enrollment system and electronically coded identification media.

Issuing Official—An official who is authorized to register individuals into the Installation Access Control System and issue IPs. Issuing officials normally work at the Installation Access Control Office.

Person Category—Individuals registered in the IACS are placed in one of 15 different person categories. Each person category has specific risk-based registration requirements and restrictions, which identifies the relationship between the individual and USAFE. One person category is for DoD ID-card holders while the remaining 14 categories are for IP applicants.

Probable Cause—Reasonable grounds supporting a charge is well-founded.

Requester—A DoD ID-card holder who requests an IP for an individual, but is not authorized to perform sponsoring-organization responsibilities. The requester status is found only in the “Personal Service Employee” and the two “Visitor” person 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.

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

Sponsoring Organization—The organization that performs IP responsibilities based on the organization's relationship to the IP applicant. Sponsoring organizations are identified for each person category. Every IP applicant and IP holder has a sponsoring organization that has responsibilities critical to the Installation Access Control Program.

Unserviceable IP or DoD ID card—Any condition or change to the card or pass that impairs the guard's ability to verify that the card or pass holder is the individual on the card or pass, or 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.