HEADQUARTERS, UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
AS HIGHEST SERVICE AUTHORITY OF THE U.S. ARMY IN GERMANY

AND THE

UNITED STATES ARMY, EUROPE
HEAD WORKS COUNCIL

CONCLUDE THE FOLLOWING

SHOP AGREEMENT

Pursuant to the provisions of Section 73, in conjunction with Section 69 and Section 75(3)17, German Personnel Representation Law (modified version).

1. PURPOSE. This shop agreement governs the use of the Enhanced Security Pedestrian Gates (ESPG), which are currently or scheduled to be installed at select pedestrian access control points (ACP) to installations throughout Germany.

2. APPLICABILITY. This shop agreement applies to all Local Nationals (LN) employees employed within Germany.

3. BACKGROUND AND TECHNICAL INFORMATION.

a. With the increasing costs from employing contract guards services, the Headquarters Department of the Army, Office of the Provost Marshal General has directed the use of electronic access control technologies to reduce the growing costs to the greatest extent possible.

b. This automated access control system identified as the Enhanced Security Pedestrian Gate (ESPG) system allows individuals currently enrolled in the Installation Access Control System (IACS) to obtain access to the installation through the ESPG using an automated verification concept. The Enhanced Security Pedestrian Gate (ESPG) is designed to reduce the requirement for contract security guards as well as detect, deter, and prevent unauthorized personnel from entering the installation using a lost or stolen ID Card. By using the Installation Access Control System (IACS) as the systems access database, the ESPG will validate whether an ID Card holder is authorized to enter the installation. The person must slide his/her ID card through the card reader slot. At that point the card reader communicates with the IACS database to determine

if the individual is enrolled in IACS and authorized on that installation. While entering thru the outer doorway, the ESPG scans to see if more than one person is attempting to enter. Once the outside door is closed, the person must place their index finger on the bio-metric reader. The system then communicates with the IACS database and compares the fingerprint presented to the image on record of the used ID Card. If they match, the door will open to the installation side allowing the person onto the installation.

1. The following conditions will halt the access process:

a. The person is not enrolled in IACS.

b. The person is either barred or not authorized to enter the installation.

c. If more than one person is detected attempting to enter the installation at the same time.

d. The fingerprint presented does not match the card swiped to enter the ESPG.

f. The fingerprint reader could not successfully read the print presented. This is usually caused by improper seeding of the finger on the bio-metric reader.

c. Key Operational Features.

1. CCTV - The ESPG is under continuous surveillance by a Closed Circuit Television (CCTV) system that is continuously recorded. Cameras, their placement, and viewing angles will vary depending on each particular location installed. The cameras will be used to observe persons approaching, using, and exiting the ESPG. The monitoring point for the cameras will normally be installed in the primary ACP guard shack however, if multiple ESPGs are installed on one site the monitoring and remote control of the systems may be consolidated into a single centralized monitoring station. Only the Provost Marshal or other designated security officials will have access to downloading or perform administrator functions on the monitoring/recording system. The monitoring and recording devices will be secure at all times. The monitoring computer operating system and CCTV monitoring system software will be password protected in accordance with U.S. Army in Europe Information Security standards. The recording systems employed as part of the total monitoring system have a recording and retrieval capability of up to approximately 30 days. After a maximum of 30 days, the recorded images will be overwritten by images recorded during the next 30 day recording cycle. There exists the capability to download the recording to a standard 3.5" micro floppy disk, writable compact disk and/or standard videotape.

2. Intercom System - The ESPG is equipped with an intercom system. Any individual may contact the ESPG guard monitoring station and request assistance or notify them of an emergency.

3. Power - If primary power is lost, there is an 8 hour back up supply so the POD will continue working. If ALL power is lost, the door that opens to the outside of the installation is immediately UNLOCKED and you can exit the POD.

4. Alarms - The ESPG is equipped with the following alarms which annunciate at the ESPG guard monitoring station:

a. Duress Alarm - Mounted inside the ESPG is a large red push button emergency alarm button. Pressing this button will generate a silent alarm that can only be heard at the guard monitoring station.

b. Fire Alarm - Mounted on the ceiling of the ESPG is a fire alarm which annunciated at the ESPG guard monitoring station. In the event of a fire alarm the system will go into fail-safe mode releasing the exterior door allowing any person to exit the ESPG out away from the installation.

c. Multiple Person / Presence Detection Alarm – Mounted on the ceiling and walls are presence detectors designed to detect the presence of more than one person. If detected the access process will halt and an alarm will be generated at the guard monitoring station. If someone falls or appears unconscious, the presence detector will signal an alarm to the Guards. The guards have a remote Key Switch to open the outer door to provide assistance.

4. AGREEMENT.

a. The CCTV monitoring systems will be used solely as a deterrent towards criminal actions and terrorist attacks, and as evidence in a criminal investigation and/or trial.

b. The system will not be utilized for monitoring a LN employee's time and attendance, or used for performance evaluations or other routine personnel management functions. At no time will the visible cameras be replaced with covert cameras.

c. Only the Provost Marshal will have access to the CCTV monitoring station equipment for set up, programming, and downloading of any required information. The monitoring systems will either be housed in a lockable cabinet and/or the system will be secured inside a room. The computer program will be password protected to restrict access. Passwords will not be shared and will be retained by the security administrator for each station. The password for the system will be changed in accordance with U.S. Army in Europe Information Security policies.

d. Recordings will be downloaded to a 3.5" micro floppy disk, writable compact disk, or videotape. The local Provost Marshal or the local security manager will determine when and what portion of any video segment is downloaded or copied. Recordings will be provided exclusively to police or other representative authorities for later use as evidence in official investigations.

e. If an event concerns LN employees, the Commanders or designated representatives of the affected agency, the works council concerned and the LN employee concerned will be notified immediately as long as notification will not interfere with an ongoing investigation. The 3.5" micro floppy disks, writable compact disks, and videotapes that are being kept for pending actions will be stored in a locked cabinet in the Provost Marshal Office. Keys to the cabinet are

kept by the Provost Marshal. With the exception of those recordings required for an investigation, copies of any recordings will be erased by the security official.

f. The Head Works Councils along with the Head Representative of Severely Handicapped Employees will be informed in a timely and comprehensive manner of any changes planned regarding the principles concerning the utilization of these monitoring systems as addressed in this shop agreement. In this case, an appropriate participation procedure will be initiated.

5. EFFECTIVE DATE, TERMINATION.

a. This shop agreement enters into effect on the date on which both parties to the agreement have affixed their signatures in paragraph 7, below.

b. This shop agreement may be terminated by either party with a notice period of three months to the end of a calendar month. This agreement stays in effect until a new agreement that regulates the above matters has been concluded.

6. OTHER AGREEMENTS.

HQ USAREUR will ensure that this agreement, in German and English, is permanently posted in a prominent place, which is accessible by all LN employees no later than one week after the implementation of this agreement.

7. SIGNATURES.

TONY WHITEHOUSE Assistant Deputy Chief of Staff, G1 (Civilian Personnel), US Army, Europe	ANDREAS ROGEL Chairman US Army, Europe Head Works Council
DATE	DATE
ALEXANDER BREHM Deputy Chairman US Army, Europe Head Works Council	HEIDI STALEY Head Representative of Severely Handicapped Employees
DATUM	DATUM

ENTERING THE INSTALLATION.

NOTE: You must be registered in IACS and authorized to access the installation to be able to use the ESPG.

Step 1: Ensure the POD is not already in use. Only one person may enter the installation at a time. If being used the Yellow "In Use" LED will be illuminated.

Step 2: Ensure you're holding your ID card / Pass so the barcode is facing the correct direction then slide it through the reader. When successfully read, the Green LED will illuminate and the outer door 1 will open.

Step 3: Enter the POD and let the door self-close. You will hear a "click" as door closes.

Step 4: Once inside with the door closed, place either your right or left index finger onto the finger print reader. Do not move it! The system will make three attempts to accurately read your print. If successful the system will signal that access has been granted and the inner door will unlock.

EXITING THE INSTALLATION

Step 1: Ensure the POD is not in use, indicated by the Yellow "In Use" LED being illuminated.

Step 2: Press the round Green button (Request to exit switch) to the right hand side of the door and in a second or two the door will unlock.

Step 3: Once inside with all the doors closed the outer door should unlock automatically. If the door doesn't unlock automatically you may press the round Green button (Request to exit switch) to the right hand side of the door and in a second or two the door will unlock.

Step 4: Push open the outer door and exit the POD

TROUBLE ENTERING

The following causes will prevent someone from opening the outer door:

1. The POD is in use or temporarily out of service.
2. If the barcode on your ID Card / pass is worn off and cannot be read.
3. The person is not authorized on the installation or not registered in IACS.
4. The cards barcode was not facing the correct direction and wasn't read.

The following causes will stop the entry process and prevent someone from opening the 2nd inner door:

1. Your fingerprint was not read correctly.
2. The fingerprint presented does not match the file record of the used ID card.
3. Multiple persons were detected trying to enter at the same time.

Emergencies: If you are in the POD and have any problem you may:

1. Press the large Red mushroom shaped Panic Alarm button located on the console. This will signal to the Guards that someone needs help.
2. Use the Intercom - Press to Talk – to speak to the Guards
3. Press the round Green button (Request to exit switch) to the right hand side of the door and in a second or two the door will unlock allowing the person to exit.