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

Army in Europe
Regulation 190-45*

6 February 2013

Military Police

Law Enforcement Reporting

***This regulation supersedes AE Regulation 190-45, 7 July 2010.**

For the Commander:

JAMES C. BOOZER, SR.
Major General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes policy for implementing AR 190-45 in Europe and must be used with AR 190-45.

Summary of Change. This revision—

● Changes references to the Office of the Provost Marshal, HQ USAREUR, to the Office of the Deputy Chief of Staff, G3, HQ USAREUR.

● Establishes separate requirements for reporting category-3 serious incidents (para 8c).

● Establishes separate requirements for the Provost Marshal Division, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, HQ USAREUR, as the final approval authority for all serious incident reports (para 8d).

● Updates the information on registering sexual offenders (para 11).

● Specifies procedures for documenting registered sexual offenders in the military police blotter (para 20).

● Provides a new section on the National Crime Information Center Warrant System (sec X).

● Updates the list of category-3 serious incidents (app C).

Applicability. This regulation applies to members of the U.S. Forces under the control of the CG, USAREUR (including USAREUR tactical units), and members of the U.S. Forces assigned to IMCOM-Europe (including United States Army garrisons).

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Supplementation. Organizations will not supplement this regulation without USAREUR G3 (AEOP-PDP-LE) approval.

Forms. This regulation prescribes AE Form 190-45B, AE Form 190-45C, and AE Form 190-45D. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at *https://aepubs.army.mil/*.

Suggested Improvements. The proponent of this regulation is the Law Enforcement Branch, Provost Marshal Division, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, HQ USAREUR (DSN 370-4953/4964/4989). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G3 (AEOP-PDP-LE), Unit 29351, APO AE 09014-9351.

CONTENTS

Figures

SECTION I
INTRODUCTION

1. PURPOSE
This regulation—

a. Prescribes policy, procedures, and responsibilities for preparing and submitting serious incident reports (SIRs).

b. Provides reporting requirements unique to the Army in Europe for category-3 serious incidents.

c. Provides reporting requirements for the—

(1) Booze It and Lose It Program.

(2) Click It or Ticket Program.

(3) Registration of sexual offenders.

(4) Incidents linked to the repeal of Don't Ask, Don't Tell.

2. REFERENCES
Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS
The glossary defines abbreviations.

4. RESPONSIBILITIES

a. The USAREUR Provost Marshal (PM) is the only designated representative of the CG, USAREUR, who may—

(1) Receive SIRs.

(2) Send SIRs to the Office of the Provost Marshal General, HQDA (OPMG).

b. United States Army garrison (USAG) directors of emergency services (DESs)/provost marshals (PMs) will—

(1) Submit SIRs to the Provost Marshal Division (PMD), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, HQ USAREUR (AEOP-PDP-LE) (sec II). This reporting requirement is in addition to the reporting requirements in AR 25-55, AR 380-5, AE Regulation 525-306, and the Privacy Act of 1974 (5 USC 552a).

(2) Notify USAG commanders when a SIR is submitted to the PMD (AEOP-PDP-LE).

(3) Refer news media queries to the servicing public affairs office.

c. Medical facility commanders will notify the nearest military police (MP) station of deaths, injuries, or illnesses reportable according to AR 190-45 and this regulation.

5. POLICY

A serious incident is an actual or alleged incident or act, primarily criminal in nature, that warrants timely reporting to the Provost Marshal Division (PMD), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, HQ USAREUR, and OPMG because of its nature, seriousness, potential for adverse publicity, or potential consequences. Appendix B provides specific instructions for preparing SIRs in Europe.

a. AR 190-45 defines category-1 and category-2 incidents.

b. Appendix C defines category-3 serious incidents that are unique to the Army in Europe.

c. Serious incidents must be reported regardless of the grade or position of the personnel involved.

d. In this regulation, "U.S. Forces" personnel include the following:

(1) All U.S. military personnel.

(2) DOD civilian employees.

(3) Family members of U.S. military personnel and DOD civilian employees.

(4) DOD contractors.

(5) Local national (LN) employees (only if the incident occurred on a U.S. Army-controlled installation).

e. If a DOD contractor or LN employee commits an offense while performing his or her duties for the U.S. Government and the incident has potential for media coverage, or if it is not reportable in a higher SIR category, the incident will be reported as a category-3 serious incident.

f. The USAREUR PM may ask USAG DESs/PMs to submit SIRs for incidents that are not normally required by AR 190-45 or this regulation to provide information to the USAREUR Command Group or OPMG. The USAREUR PM will ensure the SIRs are correctly categorized and may change the SIR category when appropriate.

g. SIRs are initial-information reports. SIRs must—

(1) Be limited to basic statements about the incident.

(2) Provide only the necessary facts about the incident.

(3) Be edited to eliminate graphic details (for example, sexual-assault descriptions, obscene language, serious-injury descriptions).

h. The following are not normally reportable by SIR, but will be reported through other channels:

(1) Operational events that are reported according to Joint Publication 6-0.

(2) Aircraft accidents and related mishaps, unless they meet other SIR criteria.

(3) Nuclear-weapon accidents and incidents (NUCFLASH, BROKEN ARROW, BENT SPEAR, and DULL SWORD).

(4) Nuclear-reactor mishaps (FADED GIANT).

(5) Chemical-agent accidents or incidents.

(6) Incidents involving foreign students.

(7) Requests from civil authorities for military support of civil-disturbance or counterterrorist operations.

(8) Incidents involving national-security crimes and deliberate security compromises. These must be reported to the nearest Army counterintelligence office as required by AR 381-12.

SECTION II
REPORTING PROCEDURES

6. SIR TRANSMISSION

a. The PMD will review, and edit if necessary, SIRs submitted by USAG DESs/PMs. The PMD will send SIRs to HQDA and other agencies. (See AR 190-45, paragraph 9-5, for the required information addressees for SIRs.)

b. USAG DESs will—

(1) Send SIRs to the PMD (AEOP-PDP-LE) in accordance with AR 190-45 and paragraph 7 of this regulation. Reporting-time limits begin when the MP station is first notified of an incident. The reporting time to the PMD will not be extended because of additional reporting requirements that IMCOM-Europe or USAG commanders may impose on USAG DESs/PMs.

(2) Not delay submitting SIRs because of incomplete information. Pertinent information known by the required submission time must be provided. If necessary, the DES/PM will submit an “add-on” or “corrected” SIR as additional information becomes available (AR 190-45, para 9-3).

7. METHODS OF SUBMISSION

a. SIRs must be encrypted using public key infrastructure (PKI) and sent by e-mail to usarmy.badenwur.usareur.list.opm-le-reports@mail.mil.

b. Copies of SIRs will be distributed in accordance with AR 190-45, paragraph 9-5.

8. REPORTING CATEGORIES

a. Category-1 Incidents. The USAG DES/PM will—

(1) Ensure category-1 SIRs are immediately reported by telephone.

(a) During duty hours, the PMD must be notified at DSN 370-4959/4964/4993 or civilian 06221-57-4959/4964/4993.

(b) After duty hours, the PMD Duty Officer must be notified at civilian 0162-2961573.

(2) Send category-1 SIRs by encrypted e-mail to the PMD (para 7a) within 12 hours after initial notification of the incident.

(3) Provide information copies to other authorities as appropriate (for example, the local staff judge advocate (SJA), United States Army Criminal Investigation Command (USACIDC), senior mission commander (SMC)).

b. Category-2 Incidents.

(1) The USAG DES/PM will—

(a) Immediately notify the PMD by telephone (a(1) above).

(b) Send category-2 SIRs by encrypted e-mail to the PMD within 24 hours after initial notification of the incident.

(c) Provide information copies to other authorities (for example, SJA, USACIDC, SMC).

(2) The USAREUR PM will forward category-2 incidents to the USAREUR Command Group within 24 hours after the MP station receives the initial report. MP official reporting channels must be used to report serious incidents.

(3) To minimize potential confusion from duplicate reporting, DESs/PMs should limit the distribution of SIRs. This does not preclude any subordinate agency from forwarding to the PMD any issue or incident that it deems appropriate.

(4) If there is any question about whether or not an incident requires a formal written category-2 SIR, the PMD must be contacted.

c. Category-3 Incidents.

(1) The USAG DES/PM will—

(a) Immediately notify the PMD by telephone (a(1) above).

(b) Send category-3 SIRs by encrypted e-mail to the PMD within 24 hours after initial notification of the incident.

(2) To minimize potential confusion from duplicate reporting, DESs/PMs should limit the distribution of SIRs. This does not preclude any subordinate agency from forwarding to the PMD any issue or incident that it deems appropriate.

(3) If there is any question about whether or not an incident requires a formal written category-3 SIR, the PMD must be contacted.

d. Final Approving Authority. The Law Enforcement Branch, PMD, has final approving authority for all SIRs.

9. MILITARY POLICE ALARM SYSTEM

The Military Police Alarm (MPA) System distributes time-sensitive information about wanted persons or property to USAG DESs/PMs, USACIDC, and U.S. Air Force law-enforcement authorities throughout the European theater. MPAs apply to one incident at a time and are valid for only 30 days.

a. USAG DESs/PMs will—

(1) Initiate, cancel, or renew an MPA message (fig 1) by sending it by e-mail to the PMD. After reviewing the message, the PMD will send it by e-mail to all USAG DESs/PMs.

---

1. TO: All Directors of Emergency Services/Provost Marshals

2. SUBJECT: Military Police ALARM

3. TYPE OF ALARM: (This is the reason for the message, for example, a stolen Government weapon.)

4. ALARM NUMBER: (This number identifies the originating MP station, using the three-letter designator in appendix D, the month the MPA message is issued (two digits), the year (four digits), and the MP station sequential alarm number for the specific month. For example, MPC-137-02-2011-1 is the first alarm issued in February 2011 by the Ansbach MP station.)

5. DESCRIPTION: (This should be a brief description of the person or item involved. It should include, as appropriate, the person's social security number and unit, the weapon serial number, the vehicle registration number, the chassis number, the license plate number or the bumper marking, and other pertinent information.)

Figure 1. Military Police Alarm Message Information

(2) Establish procedures to ensure host-nation (HN) law-enforcement authorities are informed when MPA messages are initiated, canceled, or renewed.

(3) Ensure MPA messages involving lost or stolen license plates are sent by e-mail to the USAREUR Registry of Motor Vehicles (RMV) at usarmy.badenwur.usareur.list.opm-le-reports@ mail.mil.

b. MPA messages may include but are not limited to the following:

(1) Wanted persons (including but not limited to escaped military prisoners, defectors, and suspects sought for serious offenses).

(2) Missing persons (normally missing under unusual circumstances). An MPA message will also be issued immediately on notification of a missing juvenile.

(3) Lost or stolen weapons, vehicles, and classified Government property.

c. PMs will not use MPA messages to report the following:

(1) Deserters or persons who are absent without leave (AR 190-9).

(2) Lost or stolen ID cards (DD Form 1173), ration cards (AE Form 600-702A), or passports.

NOTE: MPA messages should be sent based on the individual case, and not as a routine administrative function.

d. MP stations will maintain reference copies of MPA messages for 30 days and file them by date-time-group. To simplify MPA administration, each MP station must have a sequential log of MPAs initiated by type, number, and date. These records may be maintained in electronic format.

10. BE ON THE LOOKOUT

a. A "be on the lookout" (BOLO) is a notification issued from one law-enforcement entity to another. It typically includes information about a person who should be apprehended or detained, or a person of interest to watch for.

b. USAG DESs/PMs will—

(1) Enter BOLO information into the Centralized Operations Police Suite (COPS).

(2) Contact the PMD by telephone or e-mail and provide the contents of the BOLO.

(3) Ensure BOLO information in COPS is accessible and viewable by all USAG DESs/PMs.

c. The USAREUR PM will send an e-mail message to all USAG DESs/PMs to notify them about the COPS entry.

11. REGISTRATION OF SEXUAL OFFENDERS

a. When requesting access to an OCONUS installation, any person who has been convicted of a covered offense, as defined by DODI 1325.7, enclosure 27, or any offense that requires sexual offender registration within a person's State of residence or the State of conviction, must register with the USAG DES/PM. Noncompliance with this paragraph is punitive and may subject military offenders to nonjudicial or judicial action under the Uniform Code of Military Justice (UCMJ). Noncompliance may also subject the noncompliant individual to adverse administrative action.

b. To register a sexual offender, USAG DESs/PMs will—

(1) Complete DA Form 3975 with all information on the individual and enter the data into COPS.

(2) Report the registration as an "information blotter entry" under offense code "9Q." Paragraph 20 provides specific guidance on information that must be included in the entry.

(3) Notify the registration office of the State in which the offender is registered and the registration office of the State in which the offender was convicted of the offender's new location. If the offender was convicted by military court-martial, only the State in which the offender is registered must be notified.

(4) Notify the offender that he or she must report to the MP station when he or she receives reassignment orders.

c. Procedures for documenting registered sexual offenders in the blotter are as follows:

(1) The MP processing a sexual offender registration will complete all blocks of DA Form 3975 as follows:

(a) Block 1, Report Type: Enter "X" in the information block.

(b) Block 1g, Offense Code(s): Enter "9Q."

(c) Block 1h, Offense Description: Enter "Registration of convicted sexual offender."

(d) Section III: Enter the subject's name, grade, sex, age, Social Security number, physical description, unit of assignment, assignment address, home address, name of employing organization, and employer's unit address, if applicable.

(e) Section VI: Enter the license-plate number, make, model, and description of all vehicles registered by the offender and of any other vehicles the offender is authorized to drive.

(f) Section VII: Enter a narrative description of the offense for which the subject was convicted that requires registration; the sentencing date by court-martial or criminal-court proceedings, and any specific restrictions detailed in the sentence, such as the minimum distance between the individual's residence and schools, playgrounds, or other areas where youngsters gather. The narrative will include the following statement: "See attached court-order for additional details."

(2) The registration must be reported as an information blotter entry.

(3) DA Form 3975 must be completed as an information entry in COPS.

(4) The MP completing the DA Form 3975 will attach a copy of the court-order or sentencing document to the DA Form 3975 and forward the form to the USAG DES/PM.

12. "DON'T ASK, DON'T TELL" REPEAL INCIDENTS

a. USAG DES/PMs will report any crimes to the PMD involving or related to the repeal of "Don't Ask, Don't Tell" that affect unit operations, readiness, or mission status.

b. Crimes involving or related to the repeal of “Don’t Ask, Don’t Tell” will be treated as SIR category-3, command-interest reports.

SECTION III
SPECIAL PROGRAMS AND ASSOCIATED REPORTING PROCEDURES

13. “BOOZE IT AND LOSE IT” AND “CLICK IT OR TICKET” PROGRAMS
The USAG DESs/PMs enforce all aspects of safe driving through traffic enforcement. A key element of this enforcement is conducting the “Booze It and Lose It” and “Click It or Ticket” programs each holiday weekend. The 4-day Federal holiday weekend periods are around the birthday of Martin Luther King, Jr., President’s Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving, Christmas, and New Year’s Day. These programs reduce the number of alcohol-related driving offenses and the number of injuries suffered in traffic accidents by enforcing the requirement that all passengers wear seatbelts.

14. REPORTING REQUIREMENTS

a. Each USAG DES/PM must establish checkpoints during the holiday weekends on each installation. Off-post checkpoints will be established only after coordination with HN police. The checkpoints should be established at random times and locations throughout the weekend beginning at 1800 on the last workday before the holiday and ending at 0600 on the first workday after the holiday weekend.

b. Each USAG DES/PM will send a completed AE Form 190-45B (fig 2) to the PMD by e-mail no later than 3 workdays after the holiday weekend.

SECTION IV
ARMED FORCES TRAFFIC TICKET REPORTING REQUIREMENTS

15. DD FORM 1408
The USAG DES/PM will send a copy of each DD Form 1408 or MP report for traffic violations or accidents to the USAREUR RMV within 60 days after the date of issue. This will ensure that—

a. The information is entered into the Vehicle Registry Information Network. Properly tracking traffic-point assessments, suspensions, and revocations of drivers licenses are crucial to the management of the system.

b. Actions taken against traffic offenders are completed correctly.

c. When the suspending authority fails to respond within 60 days after receiving DD Form 1408, the USAG DES/PM or Chief, USAFE Security Forces, assesses traffic points and sends the form to the USAREUR RMV (AE Reg 190-1, para 2-21b).

“Booze It and Lose It”/“Click It or Ticket” Violation Report
(AE Reg 190-45)

1. Reporting garrison PMO	2. Begin date (YYYYMMDD)	3. End date (YYYYMMDD)
USAG Baden-Württemberg	20130118	20130121

4. Check applicable report

☐ Booze It and Lose It ☒ Click It or Ticket

Part I - Vehicles Checked

Vehicles checked by military police	Vehicles checked by host-nation police	Total number of vehicles checked
1,026	1,154	2,180

Part II - Citations Issued

Tickets issued by military police	Tickets issued by host-nation police	Total number of tickets issued
46	52	98

Part III - Offender Demographics

Number of offenders by grade		Number of offenders by age	
E1-E5	17	Under 18 years	0
E6-E9	0	18 - 25 years	35
O1-O3	3	26 - 33 years	28
O4-O5	7	34 - 41 years	14
DA civilians	0	42 - 49 years	12
Family members	4	50+ years	9
Local national employees	13	Unknown	0
Civilians	7		
Others	47		
Unknown	0		
Total offenders	98	Total offenders	98

Part IV - Offender Information

Name (last, first, MI)	Unit	Grade	Age	Date	2d offense	3d offense
Doe, Jane M.	IMCOM-Europe	LN	24	20130118	☒	☐
Smith, John W.	18th Engineer Brigade	SSG	43	20130119	☐	☒
					☐	☐
					☐	☐
					☐	☐
					☐	☐

AE FORM 190-45B, JAN 13 Previous edtions are obsolete. *ILF Vers. 01.00* ***Page 1 of 3***

Figure 2. Sample AE Form 190-45B

Part IV - Offender Information (continued)						
Name (last, first, MI)	Unit	Grade	Age	Date	2d offense	3d offense
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐

5. Remarks

Individual apprehended was a local national.
Individual apprehended was a relative.

6. Type or print name and rank	7. Signature	8. Date (YYYYMMDD)
John Doe, SSG		

AE FORM 190-45B, JAN 13 — *ILF Vers. 01.00* ***Page 2 of 3***

Figure 2. Sample AE Form 190-45B (Continued)

SECTION V
MILITARY PROTECTION ORDERS

16. MILITARY PROTECTION ORDERS

Commanders will ensure that a copy of each military protection order (MPO) issued to a Soldier is sent to the USAREUR G3 (AEOP-PDP-LE) within 5 days after it has been issued, with copies furnished to the installation Family advocacy program manager (FAPM), the chief of social work services (SWS), and the USAG DES/PM.

SECTION VI
DISPOSITION OF MILITARY POLICE REPORTS, RECORDS, AND FORMS

This section provides guidance for disposing of MP reports, records, and forms (including standard MP reports in AR 190-45 and reports required by this regulation). AR 190-45, paragraph 4-2, provides more guidance on MP reports; AR 190-45, appendix B, provides instructions for completing DA Form 3975.

17. DA FORM 3975

a. A copy of DA Form 3975 with all enclosures will be sent through the next higher headquarters to the unit commander or supervisor. When more than one subject or unit is involved, each commander or supervisor will be provided a copy of the MP report. If the subject is unknown and the unit itself is involved, the unit commander will receive a copy of the report.

b. For cases involving civilians, the USAG commander or the civilian misconduct-action authority will receive a copy of DA Form 4833 directly from the office of origin. Reports without DA Form 4833 will be sent to the commander, supervisor, or sponsor of the civilian for disposition of the offense.

NOTE: DA Form 4833 is used with DA Form 3975 to record actions taken against identified offenders and to report the disposition of offenses investigated by military and civilian law-enforcement agencies.

c. For traffic offenses, a copy of DA Form 3975 must be sent to the USAREUR RMV. One of the following documents must be sent with the form:

(1) DA Form 4833 or DD Form 1408 showing the action taken by the commander.

(2) A memorandum from the USAREUR PM with a suspense date to the commander to take action and return DA Form 4833 or DD Form 1408.

d. The original forms must be kept at the MP station. MP reports must be kept in the current files area (CFA) for at least 6 years or until no longer needed for conducting business, then retired to the Army in Europe Records Holding Area (AERHA).

18. DD FORM 1408

The USAG DES/PM will process DD Form 1408 as follows:

a. The original (white copy) will be sent to the responsible commander for action.

(1) The commander must complete the Final Report of Action Taken and return DD Form 1408 to the USAREUR RMV.

(2) A copy of the citation, with a cover letter, must be provided to the Vehicle Registration Section, USAREUR RMV, if the suspense provided to the unit commander is not met.

b. The yellow copy will be filed at the Drivers Licensing Section, USAREUR RMV.

c. The pink copy will be given to the vehicle operator or placed under the windshield wiper if the vehicle is unattended.

19. DISPOSITION OF MILITARY POLICE REPORTS, RECORDS, AND FORMS FOR GARRISONS AFFECTED BY BASE CLOSURES

The Army Records Information Management System (ARIMS) (AR 25-400-2) shows disposition instructions for military records. Most MP records must be maintained in the CFA for 6 years after the documents are closed out. After 6 years, they must be retired to the AERHA. The ARIMS website at *https://www.arims.army.mil/* provides instructions for specific records.

a. The USACIDC receives reports of criminal investigations, selected MP reports, and other related records described in the ARIMS Records Retention Schedule-Army (fig 3). These reports will be sent to the following address:

United States Army Crime Records Center
6010 6th Street
Fort Belvoir, VA 22060-5506

b. Administrative reports will be sent to the AERHA at the following address:

Army in Europe Records Holding Area
Unit 23203, Panzer Kaserne
APO AE 09263-3203

MILITARY POLICE			
Category Description	These records concern enforcement of military discipline, physical security, traffic control, control over firearms and dangerous weapons, and apprehension, restraint, confinement, administration, sentences, parole, restoration, and disposition of prisoners.		
Record Title	Criminal investigation data references - Cards sent to Crime Records Center.		
Record Description	Cards kept by Criminal Investigation Division units showing persons involved in criminal investigations. Included are DA Forms 2804 (Crime Records Data Reference).		
Disposition	TE40. Event is after date of final report. Keep in CFA until event occurs and then until no longer needed for conducting business, then retire to RHA/AEA. The RHA/AEA will destroy the record 40 years after the event.		
Event Description	40 years after date of final report		
Privacy Act Number	A0190-45DAMO	Event Driven	Yes
Disposition Authority	NC1-AU-78-78	Additional Disposition Authority	
Record Number	190-45g1	Record Type	Transfer
Permanent Record	No	Duration	40
Prescribing Directives	190-45		
Year Type	Calendar Year		

Figure 3. Military Police Records Disposition Instructions

SECTION VII
MILITARY POLICE BLOTTERS

20. DOCUMENTING INFORMATION IN THE MILITARY POLICE BLOTTER

The policy in this paragraph applies to all PMD activities. All violations of this policy will be reviewed by the USAREUR PM and referred to the respective commander for appropriate action.

a. The MP blotter (DA Form 3997) is a chronological record of police activity developed from reports, complaints, information, and incidents covering a 24-hour period that occurs in an MP station's area of responsibility. The 24-hour period starts at 0001 and ends at 2400. Events may be criminal or noncriminal. Reports of events will be entered in the blotter in accordance with AR 190-45 and this regulation. Blotter reports for the previous day will be provided to the PMD (AEOP-PDP-LE) and other recipients by 0900 each day.

b. A person will be reported in the blotter as the *subject* of an offense only when credible information exists that an offense punishable under the UCMJ, U.S. Federal law, or German law has been committed.

c. A person will be reported as a *victim* when that individual has been adversely affected by the harmful actions of someone or something as a result of a crime, accident, or other event or action. An adverse effect can also result from acts of nature such as a wind storm or hail damage.

d. A person will be reported as a *witness* when that person has seen or heard what occurred during an incident. This includes individuals who may have gained knowledge of an incident or event secondhand or through other means.

e. Blotter entries will not include the names of juvenile subjects or their parents, guardians, or sponsors. Entries will not list the names of any victims of sensitive incidents, such as a victim of a rape or child molestation. In these cases, entries must use the term *Protected Identity* where the name of the subject or victim is normally listed. A *Restricted* blotter entry is used only when a sensitive case must be controlled and has not been printed in the blotter. The blotter will indicate that the entry is *Restricted* and include the number of the associated MP report.

f. In accordance with AR 190-45, evidence collected as a result of restricted reports of sexual assault and domestic violence will be entered as an information report into COPS using an offense code from the 6Z or 9J series, respectively. The evidence will be marked with the restricted reporting control number issued by the sexual assault response coordinator (SARC)/Sexual Harassment/Assault Prevention and Response Program (SHARP) coordinator. When evidence is added or removed from the evidence room, a reference blotter entry will be made to document the activity.

g. Information that is not investigative in nature but must be entered into the blotter is recorded using a 2-series code. The second digit of a 2-series code identifies which level of command created the code. In the European theater, the letters A through J are reserved for the Army service component command, and K through Z are reserved for USAGs. Unless otherwise specified, USAGs may add to DA- and USAREUR-created codes. Additions by USAGs may expand on the code but must not change the intent of the code. For example, the code *2D1* is for lost ID cards. USAGs may further define what type of ID card was lost by adding letters or numbers to the code, for example, *2D1FM* would indicate a lost ID card of a Family member. The added information does not change the intent of the code because the code still tracks a lost ID card. Appendix E lists the offense and incident codes approved by the USAREUR PM for use by the USAG DES/PM.

21. BLOTTER DISTRIBUTION AND EXTRACTS

a. The distribution of the complete MP blotter is restricted to the following: USAG DESs/PMs, SJAs, USACIDC, garrison commanders, and SMCs/general court-martial convening authorities (GCMCAs). Distribution to the SJAs will generally be restricted to the SJA or deputy staff judge advocate (DSJA), and to the chief of justice (CoJ). The SJA, DSJA, and CoJ will redistribute as required within judge-advocate channels. The CoJ may coordinate with the USAG DES/PM for wider distribution within the office of the SJA based on an SJA-provided distribution list. Other persons who require a copy of the blotter must send a request with a justification to the PMD (fig 4).

b. Blotter extracts concerning any person listed as a subject may be provided to the subject's commander or activity director as required; distribution will be limited to the commander or activity director exercising direct supervision over the listed subject. Blotter extracts must also be provided to the responsible USAG safety office, the Army Substance Abuse Program (ASAP) coordinator, the FAPM, and the 66th Military Intelligence Brigade for incidents within their areas of responsibility and expertise.

c. PMOs will not distribute multiple MP blotter extracts to subordinate units; this is the responsibility of the commander receiving the extract. Any other distribution may be a violation of AR 190-45, the Privacy Act, or the Freedom of Information Act.

d. MP blotters, extracts of blotters, and SIRs are considered law-enforcement sensitive and must be stamped FOUO. They contain personally identifiable information (PII) and must be protected in accordance with AR 340-21 and 5 USC 552a. MP blotters must be PKI-encrypted. Failure to properly protect PII covered by the Privacy Act may result in criminal or civil penalties, as detailed in AR 340-21, paragraph 4-9.

e. MP blotter extracts of specific offenses will be provided to USAG activities that require the extracts in order to accomplish their missions. Activities requiring extracts may include the following:

(1) Local Military Intelligence Detachments (MIDs). Local MIDs require extracts pertaining to reported bomb threats, suspicious telephone calls, uncleared photography of installations or access-control points, reports of surveillance of installations, and any other acts or actions that could be considered suspicious or threats to USAGs or installations. Journal entries pertaining to the above that have not been or will not be added to the blotter must also be shared with the MIDs.

(2) Safety. The safety office will receive extracts of blotters pertaining to any entry where a Soldier, civilian employee, or Family member has been involved in an unsafe act or accident that resulted in a death or serious injury.

(3) ASAP. The ASAP coordinator will receive extracts of blotters pertaining to any incident in which drugs or alcohol were involved.

(4) SWS or SARC/SHARP. The local SWS or SARC/SHARP will receive extracts of blotters pertaining to domestic violence, child abuse, and sexual assaults by any member of the U.S. Forces (para 5d).

(5) HN Police. Blotter information may be shared with HN police when there is a U.S.-HN connection, for example, a joint investigation. USAG DESs/PMs will contact the agencies involved for further clarification as needed to provide better support both to the agencies and the USAGs. Because blotters contain PII, USAG DESs/PMs will coordinate with their servicing SJA to ensure that the information sharing is in accordance with U.S. and HN privacy laws.

(6) FAPMs. The local FAPMs will require blotter extracts pertaining to domestic violence, child abuse, and sexual assaults by any U.S. Forces member.

f. Information concerning the administration of the MP station (such as personnel changes, inspections, visitors, and other administrative data) must be recorded in the MP desk journal. The MP desk journal will not report incidents that should be entered into the MP blotter. Similarly, the blotter will not be used to document information concerning routine administrative details that should otherwise be captured in the MP desk journal.

(1) MP desk journals are used to account for patrol activities when an MP patrol is dispatched to provide support or render a service. All journal information will be recorded using the COPS journal module.

(2) The intended use of the desk sergeants journal is to record information to be used internally by the staff of the MP station and to note useful information that requires followup. For example, a driving under the influence (DUI) incident would be included in the blotter rather than listed in the journal as “awaiting breath- and blood-alcohol content (BAC) results from the *Polizei*.” Cross-referenced blotter entries will be used to provide subsequent “offense” information.

g. Only MP reports (DA Form 3975) are authorized for recording information or complaints received or observations made by the MP and to serve as a record of all investigating activity. More information on the use of DA Form 3975 can be found in AR 190-45, chapter 4.

h. Extracts from MP blotters and SIRs are considered law-enforcement sensitive information and will be marked FOUO as explained in subparagraph d above. Although the COPS database is password-protected, the transmission of information from the database by e-mail is not. PKI-compliant MP stations will encrypt all MP blotters, extracts, journals, and SIRs using PKI before they are sent to commanders or law-enforcement agencies.

i. MP blotters will be sent by e-mail to the PMD by 0900 each day, including weekends and holidays. If an MP blotter cannot be submitted by 0900, the MP station must call the PMD, at DSN 370-4959/4964/4993 or civilian 06221-57-4959/4964/4993. On weekends and holidays, the MP station must call the PMD duty officer at civilian 0162-296-1573.

(1) The service account address for MP blotters is usarmy.badenwur.usareur.list.opm-le-reports@mail.mil.

(2) When e-mail service is disrupted, MP blotters must be sent by fax. The PMD fax number is DSN 370-4948 or civilian 06221-57-4948. Once e-mail is restored, copies of blotters that were faxed must be sent by e-mail to the PMD.

Letterhead

Office Symbol Date

MEMORANDUM THRU Director of Emergency Services/Provost Marshal, USAG *xxxxxxx*, APO AE *xxxxx*

FOR USAREUR G3 (AEOP-PDP-LE), Unit 29351, APO AE 09014-9351

SUBJECT: Exception to Policy for Distribution of the Military Police Blotter

1. I request an exception to policy in AR 190-45 and AE Regulation 190-45 to allow (*name of person, grade, position, and organization*) to receive a copy of the military police (MP) blotter from the USAG *xxxxxxx* Director of Emergency Services/Provost Marshal on a recurring basis.

2. Justification. (*Reason or need for this individual to receive the blotter*.)

(**NOTE:** The individual must have some command or control relationship over all military, civilian, and Family members living or working in the area covered by the respective MP blotter or must otherwise be engaged in official business that requires routine access to law-enforcement sensitive information as part of their official duties. The periodic need for blotter information is not a justification for recurring distribution.)

3. I certify that this individual has been appointed by (*the GCMCA*) as the (*summary court-martial convening authority*) and has jurisdictional responsibility over the USAG *xxxxxx* area of operations, which requires receipt of the entire MP blotter on a daily basis.

4. The POC for this action is (*POC name and telephone number*).

USAG commander

Figure 4. Military Police Blotter Request Format

SECTION VIII
LAW ENFORCEMENT AND DISCIPLINE REPORT

22. SUBMISSION PROCEDURES FOR THE LAW ENFORCEMENT AND DISCIPLINE REPORT

USAG DESs/PMs must submit AE Form 190-45C (fig 5) to the PMD (AEOP-PDP-LE/Senior Program Manager) by the 10th workday of the month.

Law Enforcement and Discipline Report
(AE Reg 190-45)

Period 20120101 **Thru** 20120331	**QTR FY** 2 FY 12	**To** USAREUR G3 (AEOP-PDP-LE) Unit 29351 APO AE 09014-9351	**From** Cdr, USAG Baden-Württemberg 29237 APO AE 09102-9237

Part I - Strength

a. Avg U.S. Army personnel 5	**b. Avg Family member** 10	**c. Avg other service** 8
d. Avg Department of the Army civilian 3	**e. Avg other** 0	**f. Avg total population** 26

Part II - Crimes against persons

	Type of offense	Founded offenses						Identified offenders: U.S. Army personnel						Identified offenders: Others				Alcohol in-volvement	Total
		Army subjected on post	Army subjected off post	Other subjected on post	Other subjected off post	Subjected unknown on post	Subjected unknown off post	R	M	N	C	H	X	Army FM	DAC	Other Svc	Others		
	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	k.	l.	m.	n.	o.	p.	q.	r.	b.- q.
1.	Murder						2										2	2	4
2.	Robbery	4									1			2	1				8
3.	Aggravated assaults	2						1		1									4
4.	Simple assaults	2										2							4
5.	Other																		
	Part III - Drug crimes																		
	Use/possession																		
6.	Narcotics	5																	5
7.	Dangerous drugs																		
8.	Marijuana																		
	Sale/distribution																		
9.	Narcotics																		
10.	Dangerous drugs																		
11.	Marijuana	5							1		1					1	2		10
12.	Other																		
	Part IV - Sex crimes																		
13.	Rape	1						1										1	2
14.	Other																		
	Part IV - Crime against property																		
15.	Burglary/housebreaking	4															4		8
16.	Auto theft	1													1			1	2
17.	Arson																		
18.	Other																		

AE FORM 190-45C, MAR 08 Previous editions are obsolete. *Vers. 01.00* ***Page 1 of 1***

Figure 5. Sample AE Form 190-45C

SECTION IX
MILITARY POLICE BACKGROUND CHECKS

AR 190-45, paragraph 2-6, provides policy on processing MP background checks. Information on disclosing information can be found in AR 190-45, paragraph 2-6; and AR 340-21, paragraphs 2-1, 3-1, and 3-2.

23. MILITARY POLICE BACKGROUND-CHECK REQUESTS

The COPS Military Police Reporting System (MPRS) is a database that contains all MP reports filed worldwide. Many organizations, agencies, and individuals are required to complete an MP background check for employment, installation access, security clearances, and other purposes as required by Army and Army in Europe regulations. Individuals may request an MP background check for individual purposes, for example, passport applications. The USAG DES/PM will—

a. Appoint two staff members (a primary and an alternate) to process the MP background checks conducted by the USAG PMO.

b. Receive and screen all requests for MP background checks on official forms including DD Form 369, DA Form 7281, and AE Form 195-45D.

(1) Requesters must have a current authorization memorandum from their agency on file with the USAG DES/PM. Sponsoring agencies will update the authorization memorandum once a year or as changes occur (fig 6).

(2) Individuals requesting an MP background check on themselves only must present valid photo identification (for example, official passport, DOD ID card).

c. Use the MPRS COPS name-check tools to process all requests for MP background checks (AR 190-45, para 2-6d).

d. Securely distribute all requests and results for MP background checks submitted to the USAG DES/PM (AR 190-45, para 2-6a, and AR 340-21, paras 2-1, 3-1, 3-2, 3-3, and 3-4).

e. Maintain a record of and provide quality assurance for the processing of MP background checks and all MP background-check transactions conducted at the USAG DES/PM (AR 190-45, para 2-6g, and AR 340-21, para 3-4).

Office Symbol Date

MEMORANDUM FOR (*the name of the servicing USAG DES/PM*)

SUBJECT: Designation of Authorized Agency Requesters of Military Police Background Checks

1. The following individuals are designated as authorized requesters for (*the name of the organization*):

Full Name	Position	Grade	Official E-mail Address

2. This memorandum expires in 1 year or earlier if changes occur.

3. The POC is (*name, telephone number, and e-mail address*).

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

Figure 6. Sample Authorized Agency Request Format

SECTION X
NATIONAL CRIME INFORMATION CENTER (NCIC) WARRANT SYSTEM

24. GENERAL

PMD personnel who have access to and use the NCIC Warrant system must be thoroughly familiar with all aspects of the warrant formats, hit confirmations, locations, hot files, and warrant cancellation policies and procedures. The PMD bears full responsibility for ensuring that the law-enforcement data-communication network and any criminal history record information received through that network will be used solely for the administration of criminal justice and law enforcement. NCIC checks will be conducted solely for law-enforcement purposes. The NCIC Warrant system will not be used for general or administrative background checks or investigations.

a. The PMD will establish rules and regulations governing access to, security of, and operation of the data-communication network and any criminal justice record information received through that network. These rules and regulations will be consistent with Federal law.

(1) All identified authorized users will be responsible for the physical security of their work terminals. Only the supervisor, system specialist, network specialist, or authorized repair technician are permitted to repair, reboot, connect, disconnect, tamper with, or attempt to install or uninstall any cables, lines, features, hardware, or software.

(2) Authorized users are responsible for the security of information received through the network, including incident details, warrant hits, reporting-party information, and information messages. Information received through the network will not be released over the telephone to the media, the public, any unauthorized attorney, or other private citizen.

(3) Authorized users may release information received through the network to the following personnel, when required for their duties as part of an official investigation or enforcement action:

(a) USAG DES/PM or a designee.

(b) SJA and the SJA's designee (generally the DSJA, CoJ, or trial counsel).

(c) USACID special agents.

(d) Military police investigators.

(e) Naval Criminal Investigative Service agents.

(f) Air Force Office of Special Investigations investigators.

(4) In addition to the users listed in (3) above, commanders and their designees, including investigating officers (IOs) appointed in writing, may also receive information through the network. Commander-appointed IOs (AR 15-6 IOs) will provide a copy of their appointment orders to the authorized user releasing the information. The orders must clearly state that the IO is investigating suspected criminal misconduct.

(5) Unauthorized individual military members, DOD civilians, private citizens, contractors, and other personnel are not authorized to receive NCIC information about stolen vehicles, regardless of whether the vehicle is listed as "stolen" or "clear." No information concerning registered owners will be provided to these individuals.

(6) Information obtained from the NCIC terminal is considered FOUO (Law Enforcement) and may not be used for anything other than official law-enforcement purposes or other purposes specifically authorized by law or regulation. Any operators found to have misused the NCIC terminal or data obtained from the NCIC terminal, for any reason, may be subject to administrative disciplinary action. Military personnel may also be subject to nonjudicial or judicial action. In accordance with AR 340-21, individuals misusing the NCIC system may also face Federal criminal sanctions.

b. In the event that the terminal area coordinator (TAC) receives information concerning an active warrant as a result of a system inquiry, the TAC will immediately provide the following information to the requester:

(1) Notification that the warrant is confirmed or unconfirmed, as applicable.

(2) The agency with jurisdiction for the warrant.

(3) The type of offense for which the warrant was issued.

(4) The name, date of birth, physical description of the person for whom the warrant has been issued.

(5) Extradition information, as applicable.

c. If a "hit" has been confirmed and the officer confirming the hit determines that local charges against the subject exist, the officer will inform the originating agency identifier (ORI) of the local charges and the disposition of the wanted subject.

d. When confirming a warrant, the TAC will inform the agency holding the warrant of the agency the TAC represents (for example, "This is the USAREUR Provost Marshal Division."). The TAC will also confirm whether or not there is an extradition request.

e. Once confirmed, the TAC will print a copy of the warrant hit, including the operator number, the name and telephone number of the person who confirmed the warrant, any additional warrant hits, and any additional information obtained through the NCIC system. The TAC will also complete a supplementary narrative report form, send all information to the requester, and keep a copy of the information on file in the Law Enforcement Branch, PMD.

f. Verification of the status of a Soldier named in an NCIC warrant is governed by the following:

(1) AR 27-40, paragraph 2-2 (governing service of criminal process inside the United States).

(2) AR 27-40, paragraph 2-4 (governing service of criminal process outside of the United States).

(3) AR 630-10, chapter 7 (surrender to civilian law-enforcement officials).

(4) NATO Status of Forces Agreement and the appropriate supplemental agreement in effect in the country in which the Soldier is stationed.

g. To request information regarding a warrant, the requester will contact the Soldier's unit or DOD civilian employee's place of duty in order to verify the individual's duty status (for example, present for duty) through the first-line supervisor. ***The requester will not notify the supervisor of the existence of a warrant in the NCIC system.*** Requesters will ask only about the current duty status of the individual in question. The requester will also notify the TAC of the status of the individual before confirming the status of a hit. During the confirmation of the warrant, the TAC will tell the ORI that the subject is not in custody and that the ORI should not take any action. ***No action will be taken to serve the warrant or conduct an arrest based on an NCIC warrant without prior coordination with the Office of the Judge Advocate, HQ USAREUR.***

25. NCIC AUTHORIZED USERS STANDARDS OF DISCIPLINE

a. In accordance with NCIC security policy, all authorized users will submit to an initial criminal history check and an additional criminal history check every 5 years.

b. Any authorized users currently under investigations for a violation of the UCMJ or Federal law, or found to have committed any felony during their term or period of employment, will have their access to the NCIC system suspended pending investigation.

26. TERMINAL AGENCY COORDINATORS

a. All USAG DESs/PMs with access to terminals connected to the NCIC network must appoint a USAG TAC. The USAG TAC is responsible for ensuring that the agency's policies governing terminal operations are consistent with PMD and Federal requirements. The USAG TAC will be appointed in writing and be the only individual authorized to conduct NCIC checks on individuals, vehicles, and weapons. Only MP Soldiers (career-management field 31) in the grade of sergeant first class or above, MP commissioned officers in the grade of captain or above, and civilian employees assigned to the USAG DES/PM in the grade of GS-11 or above may be appointed as USAG TACs.

b. The TAC will—

(1) Train terminal operators and other personnel in NCIC network operations and will develop a standing operating procedure to implement procedures for using NCIC terminals. The TAC is responsible for ensuring that all terminal operators comply with NCIC policy and procedures.

(2) Liaise with both administrative and operations personnel to ensure that all parties can fully utilize the capabilities of the NCIC system and to ensure compliance with procedures governing requests for information from the NCIC system, as established by the PMD. As a minimum, requests for NCIC checks must be processed according to the following procedures:

(a) All NCIC requests will be documented on the PMD NCIC form.

(b) If the NCIC request is made through a USAG DES/PM, the USAG DES/PM must approve and sign the request before forwarding it. NCIC requests from other agencies will be signed and approved by the requesting agency supervisor.

(c) NCIC requests internal to the PMD will be signed and approved by the requesting PMD branch chief or the Deputy Provost Marshal, USAREUR.

(d) All NCIC requests will be sent to the PMD at usarmy.badenwur.usareur.list.opm-le-reports@mail.mil.

(3) Ensure the quality and timeliness of monthly validations of wanted/missing persons and stolen/missing property records entered into NCIC computerized files.

(4) Verify the cancellation of all entries that are no longer valid.

(5) Verify that all records requiring modification are completed and supplemental records are created if entries require it.

(6) Complete the validation certification/completion form on the NCIC terminal according to NCIC procedures.

(7) Route and distribute NCIC operations bulletins, manuals, and other publications to the appropriate personnel and units throughout USAREUR.

(8) Ensure that procedural formats and codes established by this regulation and the NCIC manual are strictly adhered to in order to ensure that—

(a) PII and other private information is protected in accordance with the Privacy Act.

(b) Information obtained from the NCIC system is not released to unauthorized personnel.

(c) Only authorized users are permitted to operate NCIC terminals.

(d) “Hot files” are entered, modified, and purged in accordance with the NCIC manual.

27. NCIC TERMINAL OPERATORS (TOs)

NCIC TOs will—

a. Annotate all criminal history checks in the NCIC log and ensure that individuals requesting the information sign the log if they receive a printed copy of the information. NCIC terminals are restricted-access terminals and may not be accessed by any individual not trained in how use NCIC terminals and not listed on the NCIC access roster.

b. Maintain their TO certification and be retested every 2 years.

c. Ensure that the NCIC operator’s manual, which must be handled as part of the terminal system, is properly handled as FOUO material and stored in accordance with AR 380-5.

d. Maintain a usage log for the NCIC terminal by tracking all requests for use and actual usage by name of the user, date and time of the usage, and subject.

28. CRIMINAL HISTORY REQUESTS

The NCIC system may be used to process requests for criminal history checks only for the following:

a. As part of an ongoing criminal investigation. TOs will key-log the search with a “c” code (criminal justice).

b. For an individual seeking employment as a member of a law-enforcement agency, as a security guard, or with a fire department. The potential employee should sign a waiver authorizing the criminal history check. TOs will key-log the search with a “j” code (criminal justice employment).

c. For military Servicemembers under investigation when the investigation is likely to lead to a court-martial. In these cases, the serving CoJ or trial counsel will provide the operator with a written request. TOs will key-log the search with a “c” code (criminal justice).

d. For a civilian employee under criminal investigation when the investigation is likely to be handed off to the Department of Justice (DOJ) for action, either under the Military Extraterritorial Extradition Act or based on a DOJ determination that the criminal acts are inherently extraterritorial. Such a request should be coordinated with the CoJ, trial counsel, or international law attorney responsible for coordination with DOJ. TOs will key-log the search with a “c” code (criminal justice).

e. For an individual who is requesting registration of a privately owned firearm. TOs will key-log the search with an “f” code (firearms).

f. For an individual who is a registered sexual offender. This check should not be completed until the DA Form 3975 documenting the registration is complete. TOs will key-log the search with a “c” code (criminal justice). If a USAG commander has credible evidence providing reason to believe that an individual is a registered sexual offender who has failed to properly register with the USAG DES/PM, the USAG commander may—

(1) Order an investigation to confirm or deny this allegation.

(2) Request that the USAREUR TAC conduct a criminal history check of the individual. Criminal history checks of suspected non-registration will not be conducted below the PMD level.

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

Privacy Act of 1974 (5 USC 552a)

Adam Walsh Child Protection and Safety Act of 2006

Uniform Code of Military Justice (Manual for Courts-Martial, 2012 Edition)

Joint Publication 6-0, Joint Communications System

DOD Instruction 1325.7, Administration of Military Correctional Facilities and Clemency and Parole Authority

AR 25-52, Authorized Abbreviations, Brevity Codes, and Acronyms

AR 25-55, The Department of the Army Freedom of Information Act Program

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 27-40, Legal Services Litigation

AR 190-9, Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies

AR 190-27, Army Participation in National Crime Information Center

AR 190-45, Law Enforcement Reporting

AR 340-21, The Army Privacy Program

AR 380-5, Department of the Army Information Security Program

AR 381-12, Threat Awareness and Reporting Program

AR 630-10, Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings

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

AE Regulation 525-306, OPREP-3 Procedures: Nonnuclear Event or Incident Report

National Crime Information Center (NCIC) 200 Operator's Manual

NCIC Security Policy

SECTION II
FORMS

DD Form 369, Police Record Check

DD Form 1173, United States Uniformed Services Identification and Privilege Card

DD Form 1408, Traffic Ticket, Armed Forces

DA Form 2028, Recommended Changes to Publications and Forms

DA Form 2804, Crime Records Data Reference

DA Form 3975, Military Police Report

DA Form 3997, Military Police Desk Blotter

DA Form 4833, Commander's Report of Disciplinary or Administrative Action

DA Form 7281, Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record

AE Form 190-45B, "Booze It and Lose It"/"Click It or Ticket" Violation Report

AE Form 190-45C, Law Enforcement and Discipline Report

AE Form 190-45D, Military Police Record Check

AE Form 600-702A, U.S. Forces Ration Card

APPENDIX B
SPECIAL INSTRUCTIONS FOR PREPARING ARMY IN EUROPE SERIOUS INCIDENT REPORTS

B-1. SPECIFIC ITEMS

AR 190-45 provides the format for serious incident reports (SIRs). The following additional instructions apply to SIRs in Europe.

a. Subject Line. The subject line must include the three-letter location designator (app D) of the military police (MP) station reporting the incident. This prefix will be placed immediately before the six-digit number identifier (for example, MPC-137 930001).

b. Paragraph 6. In paragraph 6, the subject and victim sections must include the information required by AR 190-45, including—

(1) The sponsor's unit if the subject or victim is a Family member.

(2) The status of the subject or victim (for example, admitted to the hospital, at large, confined).

NOTE: SIRs must not compromise classified information by including information on individuals, units, or locations that may identify the mission of special or classified units.

c. Paragraph 7. In paragraph 7, enter a complete description of the incident. When applicable, reports about incidents on U.S. installations or in U.S. facilities involving individuals not associated with the U.S. Army must include a brief explanation as to why these individuals were on the installation or in the facility (for example, club employee, taxi driver, guest). Paragraph 7 must also indicate whether or not any of the individuals involved (subjects or victims) have been deployed at any time within the past year.

B-2. SPECIAL INSTRUCTIONS

a. SIRs involving traffic fatalities or other deaths must include the following information:

(1) The location and time of death and the attending medical authority who pronounced the death.

(2) The probable cause of death.

(3) The medical facility admitting the deceased.

(4) A statement as to whether or not an autopsy was performed or is planned.

(5) A statement as to whether or not alcohol or drug involvement is suspected.

(6) A statement as to whether or not seatbelts were worn or protective headgear was used.

b. Injuries must be identified in simple terms. The condition of hospitalized patients will be reported as *good*, *fair*, *serious*, or *critical*.

c. When a traffic accident meets SIR requirements, as much information as possible should be provided about the vehicle, driver, vehicle damage, and personal injuries. This includes the following:

(1) Individuals will be identified after their names in reference to how they relate to the incident (for example, John Smith (operator of vehicle 1), Laurie Jones (passenger inside vehicle 1), Julie Williams (pedestrian)).

(2) Property damage and suspected offenses related to the accident (for example, speeding, drunk driving, unauthorized dispatch, unlicensed operator, unregistered vehicle).

(3) Vehicle ownership.

d. Reports of controlled-substance offenses must include—

(1) The quantity of each controlled substance involved.

(2) The disposition of the controlled substance (for example, released to the United States Army Criminal Investigation Command, released to German authorities).

e. Reports of lost, stolen, or recovered property must include the following:

(1) An accurate property description. U.S. Government property descriptions will include nomenclatures and model numbers (for example, M1A1 (Abrams tank)).

(2) Serial or lot numbers of firearms or ammunition, if known.

(3) Circumstances of the loss, larceny, or recovery.

f. Reports of intrusion into a restricted area or arms room must include the following information:

(1) The nature of the restricted area.

(2) The means by which the intrusion was attempted or accomplished.

(3) The security measures in effect at the time of the incident.

(4) The reason why security measures failed, if known.

(5) The loss or damage incurred.

g. Garrison commanders will obtain approval from local military-intelligence authorities before listing sabotage or terrorist activities as a reason for destruction of U.S. Government property.

h. The use of abbreviations in SIRs is encouraged, but must be in compliance with AR 25-52 and the online glossary of abbreviations in the Army in Europe Library & Publishing System at *https://aepubs.army.mil/*.

APPENDIX C
SERIOUS INCIDENT REPORTS

C-1. GENERAL

This appendix prescribes reporting procedures for the three categories of incidents that USAREUR leaders regard as serious incidents, and provides reporting procedures for preparing serious incident reports (SIRs) for each category. The categories of incidents are—

a. Category 1 (para C-3).

b. Category 2 (para C-4).

c. Category 3 (para C-5).

C-2. ALL CATEGORIES OF SERIOUS INCIDENTS

All categories of serious incidents must be immediately reported to the Law Enforcement Branch, Provost Marshal Division (PMD), G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, HQ USAREUR, at DSN 370-4959/4964 (during normal duty hours) or civilian 0162-296-1573 (after duty hours). In all cases, the individual reporting the serious incident must follow up by sending a written report by e-mail to the PMD at usarmy.badenwur.usareur.list.opm-le-reports@mail.mil within 24 hours after reporting the incident by telephone. Additional reporting requirements for the various categories of serious incidents are prescribed in paragraphs C-3 through C-5.

C-3. CATEGORY-1 SIRs

Category-1 serious incidents are defined in AR 190-45, paragraph 8-2, and must be immediately reported to the PMD at DSN 370-4959/4964 (during normal duty hours) or civilian 0162-296-1573 (after duty hours). The individual reporting the incident must follow up by sending a written report to the PMD by e-mail at usarmy.badenwur.usareur.list.opm-le-reports@mail.mil within 12 hours after reporting the incident by telephone.

C-4. CATEGORY-2 SIRs

Category-2 serious incidents are defined in AR 190-45, paragraph 8-3, and must be reported to the PMD by e-mail at usarmy.badenwur.usareur.list.opm-le-reports@mail.mil within 24 hours after being discovered or after the PMD has been notified of the incident.

C-5. CATEGORY-3 SIRs

a. Category-3 serious incidents must be immediately reported to the PMD by telephone at DSN 370-4959/4964 (during regular duty hours) or civilian 0162-296-1573 (after duty hours). Within 12 hours after reporting the incident by telephone, the individual reporting the incident must follow up by sending a written report to the PMD by e-mail at usarmy.badenwur.usareur.list.opm-le-reports@mail.mil.

b. The following is a list of USAREUR-specific incidents that are considered category 3 and that must be reported according to the guidance in subparagraph a above. This list is not all-inclusive. Commands should report any incident that could be a serious incident for USAREUR. If any uncertainty exists considering the seriousness of the incident, commands should report it.

(1) Theft, loss, or suspected theft of, or unaccounted for or recovered—

(a) Government arms, ammunition, and explosives in quantities that do not warrant being reported as a category-2 serious incident (AR 190-45, para 8-3.h).

(b) Privately owned firearms or ammunition.

(2) Theft, suspected theft, wrongful appropriation, or willful destruction of Government-owned or -leased vehicles not otherwise considered to warrant a category-1 SIR (AR 190-45, para 8-2) or a category-2 SIR (AR 190-45, para 8-3).

(3) An incident in which a member of the military police (MP) or the United States Army Criminal Investigation Division (CID), a customs agent, or a contract-security guard (including incidents involving vehicular accidents and active-barrier systems) is titled as the subject while on duty.

(4) An accidental or negligent discharge of a firearm (Government or private) outside of a clearing barrel.

(5) Rape, sexual assault, or any other Article 120, UCMJ, crime involving a member of the U.S. Forces as either the subject or victim.

(6) Any other incident or unusual circumstance that the USAREUR Provost Marshal determines to be of concern to HQ USAREUR based on the nature, gravity, or potential for adverse publicity.

(7) Black-market activity involving five or more subjects or involving U.S. tax-free merchandise with a retail value in excess of $5,000.

(8) Any major fire or natural disaster resulting in property damage to any DOD-owned or -controlled real estate (buildings or facilities), including military personnel housing. Any property damage that results in displacement of U.S. Forces Personnel on or off post.

(9) Any incident involving U.S. Forces personnel who are unaccounted for or missing for an abnormal or unusual period of time, or whose disappearance occurred under abnormal or unusual circumstances.

(10) Any incident of misconduct involving commissioned officers who are lieutenant colonels or higher, or involving noncommissioned officers who are first sergeants or higher.

(11) Antiterrorism or force-protection incidents, issues, or concerns that occur in or relate to the Heidelberg, Stuttgart, or Wiesbaden communities.

(12) Any change in MP unit status resulting in, or likely to result in, a significant degradation to the unit's ability to accomplish its mission.

(13) Any serious injury, including any injury that results in hospitalization, of any on duty MP, CID, or customs personnel.

(14) Any use of force—

(a) Involving firearms, tasers, batons, or pepper spray by MP, CID, or customs personnel.

(b) By contract security guards in the line of duty.

(15) Any investigation involving a general or flag officer or member of the Senior Executive Service.

APPENDIX D
THREE-LETTER LOCATION DESIGNATORS FOR MILITARY POLICE STATIONS

The following three-letter location designators are used to identify military police stations by country:

BALKANS	
KOS	Kosovo
TUZ	Tuzla
BELGIUM	
BEL	Belgium
BULGARIA	
BUL	Bulgaria
GERMANY	
ANS	Ansbach
BAB	Babenhausen
BAM	Bamberg
BAU	Baumholder
DAR	Darmstadt
GAR	Garmisch
GRF	Grafenwöhr
HAN	Hanau
HDG	Heidelberg
HOH	Hohenfels
KSN	Kaiserslautern
MAN	Mannheim
SCH	Schweinfurt
STU	Stuttgart
VIL	Vilseck
WIE	Wiesbaden
ITALY	
LIV	Livorno
VIC	Vicenza
THE NETHERLANDS	
SHN	Schinnen
POLAND	
POL	Poland
ROMANIA	
ROM	Romania

APPENDIX E
2-SERIES OFFENSE AND INCIDENT CODES AND DESCRIPTIONS

The following are the only 2-series offense and incident codes approved by the USAREUR Provost Marshal for use by United States Army garrison provost marshal offices:

Offense or Incident Code	Offense or Incident Description
2B1	Surveillance - on post
2B2	Surveillance - off post
2D1A	Stolen military ID card
2D2A	Stolen installation pass
2D3A	Stolen DOD civilian ID card
2D4A	Stolen dependent ID card
2D5A	Stolen DOD contractor ID card
2D6A	Stolen retired ID card
2F1	Noise complaint
2G1	Verbal domestic disturbance
2H1	Care and control of pets
2I1	Child supervision policy
2J1A	Office lockout
2J1B	Vehicle lockout
2J1C	Vehicle lockout - unable to gain entry
2J1D	Quarters lockout
2J1E	Quarters lockout - unable to gain entry
2J1F	Barracks lockout
2J1G	Barracks lockout - unable to gain entry
2J1H	Post-lodging lockout
2J1I	Post-lodging lockout - unable to gain entry
2C1	Found property (describe)
2A1F	Fire alarm
2A1A	Arms room alarm
2A1B	Bank alarm
2A2	Unsecured building
2A3E	Medical emergency
2A4E	Emergency-vehicle escort
2A5	Money escort
2L1	Pond Security badge
2L1A	Lost Pond Security badge
2L1B	Lost Pond Security ID card
2P1	Pre-TALON report
2P1A	Suspicious package
2P1B	Suspicious person observing an installation
2P1C	Suspicious vehicle in the vicinity of an installation

Offense or Incident Code	Offense or Incident Description
2M1	Lost USAREUR license plate
2M2	Stolen USAREUR license plate
2M3	Damaged or mutilated USAREUR license plate
2N1	Lost USAREUR drivers license
2N2	Stolen USAREUR drivers license
2U1	Lost passport (U.S. official)
2U2	Stolen passport (U.S. official)
2U3	Lost passport (U.S. tourist)
2U4	Stolen passport (U.S. tourist)
2O1	Lost passport (other issuing country)
2O2	Stolen passport (other issuing country)
2A2L	Lost AAFES fuel card
2A2S	Stolen AAFES fuel card

GLOSSARY

AAFES	Army and Air Force Exchange Service
AE	Army in Europe
AEA	Army Electronic Archive
AEPUBS	Army in Europe Library & Publishing System
AERHA	Army in Europe Records Holding Area
AR	Army regulation
ARIMS	Army Records Information Management System
ASAP	Army Substance Abuse Program
BOLO	be on the lookout
CFA	current files area
CG, USAREUR	Commanding General, United States Army Europe
CoJ	chief of justice
COPS	Centralized Operations Police Suite
DA	Department of the Army
DES	director of emergency services
DOD	Department of Defense
DODDS-Europe	Department of Defense Dependents Schools-Europe
DOJ	Department of Justice
DSN	Defense Switched Network
DSJA	deputy staff judge advocate
FAPM	Family advocacy program manager
GS	general schedule
HN	host nation
HQDA	Headquarters, Department of the Army
HQ USAREUR	Headquarters, United States Army Europe
ID	identification
IMCOM-Europe	United States Army Installation Management Command, Europe Region
IO	investigating officer
LN	local national
MID	military intelligence detachment
MP	military police
MPA	military police alarm
MPO	military protection order
MPRS	Military Police Reporting System
NATO	North Atlantic Treaty Organization
NCIC	National Crime Information Center
OCONUS	outside the continental United States
OPMG	Office of the Provost Marshal General, Headquarters, Department of the Army
ORI	originating agency identifier
PKI	public key infrastructure
PM	provost marshal
PMD	Provost Marshal Division, G34 Protect Directorate, Office of the Deputy Chief of Staff, G3, Headquarters, United States Army Europe
POC	point of contact
RHA	records holding area
RMV	registry of motor vehicles
SARC	sexual assault response coordinator

SHARP	Sexual Harassment/Assault Prevention and Response Program
SIR	serious incident report
SJA	staff judge advocate
SMC	senior mission commander
SWS	social work services
TAC	terminal area coordinator
TO	terminal operator
UCMJ	Uniform Code of Military Justice
U.S.	United States
USACIDC	United States Army Criminal Investigation Command
USAFE	United States Air Forces in Europe
USAG	United States Army garrison
USAREUR	United States Army Europe
USAREUR G3	Deputy Chief of Staff, G3, United States Army Europe
USC	United States Code