

Army Regulation 190–45

Military Police

Law Enforcement Reporting

**Headquarters
Department of the Army
Washington, DC
27 September 2016**

UNCLASSIFIED

SUMMARY of CHANGE

AR 190-45

Law Enforcement Reporting

This major revision, dated 27 September 2016--

- o Adds a requirement for chain of command notification by law enforcement within 4 hours upon apprehension or initiation of investigation of a Soldier (para 1-4g(16)).
- o Updates installations' geographical area of responsibilities (table 1-1).
- o Establishes policy pertaining to the level of security clearance and background check required to use the system-generated DA Form 190-45-SG (Army Law Enforcement Reporting and Tracking System (ALERTS)) (para 2-1d).
- o Updates the policy on sex offenders on Army installations (para 2-7).
- o Updates the policy pertaining to the collection of deoxyribonucleic acid samples from Soldiers (para 2-8).
- o Updates the policy pertaining to the disclosure of information contained in military police reports or military police investigation reports (para 3-7).
- o Adds reporting requirement of domestic incidents to the Army Family Advocacy Program (para 3-9).
- o Establishes the procedure for sending a redacted version of a Law Enforcement Report to outside agencies (para 4-2e).
- o Adds guidance on preparing and disseminating DA Form 4833 (Commander's Report of Disciplinary or Administrative Action) (para 4-7).
- o Establishes a requirement for all installations to use the DA Form 190-45-SG, also known as ALERTS, to generate a blotter report (para 7-15a).
- o Updates the serious-incident report requirement (para 8-1).
- o Changes the status for incidents involving biological select agent and toxins, from a category 2 serious incident to a category 1 serious incident (para 8-1i).
- o Clarifies serious-incident report requirements for deaths occurring on and off post (para 8-3m).
- o Establishes procedures for suspicious activity reporting (para 8-7).
- o Adds a law-enforcement-sensitive statement to all serious-incident report notifications (para 9-1).

- o Clarifies the completion of serious-incident reports that involve protected identities (para 9-4).
- o Authorizes the limited use of the Federal Bureau of Investigation's National Crime Information Center to conduct checks of visitors to an installation (para 12-2).
- o Establishes a procedure for reporting positive drug urinalysis results into the National Instant Checks System database (para 12-4).
- o Adds offense codes pertaining to Articles 112a, 120, and 134, Uniform Code of Military Justice (table C-1).
- o Changes phencyclidine's classification from dangerous drug to hallucinogen (table C-1).
- o Updates offense codes that pertain to suicide, including suicide attempts (table C-1).
- o Adds offense codes to register Department of Defense employee and Family members or dependents who are sex offenders (table C-1).
- o Incorporates policies from Army Directive 2013-06, which is hereby rescinded (throughout).

PREFACE

DA Form 190-45-SG is a system-generated form, which is also referred to as the Army Law Enforcement Reporting and Tracking System (ALERTS).

Effective 27 October 2016

Military Police

Law Enforcement Reporting

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation establishes policies and procedures for offense and serious-incident reporting within the Army; for reporting to the Department of Defense and the Department of Justice, as appropriate; and for participating in the Federal Bureau of Investigation's National Crime Information Center, the Department of Justice's Criminal Justice Information System, the National Law Enforcement Telecommunications System, and State criminal justice systems. It implements the reporting requirements of DODI 7730.47, the sex offender registration requirements of DODI 1325.07, and the victim/witness requirements contained in DODI 1030.2. It implements the portion of Section 1561a, Title 10, United States Code (The Armed Forces Domestic Security Act) that gives a civilian protection order the same force and effect on a military installation that it has within the jurisdiction that issued it. This regulation mandates the use of DA Form 190–45–SG (Army Law Enforcement Reporting and Tracking System (ALERTS)), a system-generated form. It sets forth the revised objectives and procedures applicable to the referral and trial by U.S. magistrates for misdemeanors committed on Army installations. It also

describes the proper use, preparation, and disposition of the Central Violations Bureau (CVB) Form (United States District Court Violation Notice) when referring offenders to the U.S. Magistrate. It meets law enforcement reporting requirements for selected criminal incidents and provides law enforcement agencies, such as the Department of Homeland Security and Transportation Security Administration, with the most current information available. It also provides the chain of command with timely information to respond to queries from the Department of Defense, the news media, and others.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to Department of the Army civilian police and security guard activities. This regulation is required during mobilization. Chapters 10–12 apply to misdemeanor offenses committed on United States Army installations in the United States and its territories that have a U.S. Magistrate Court. Chapters 10–12 apply to U.S. Army military police, directorates of law enforcement and security, Department of the Army civilian police and security guard activities, and to security force operations when authorized to issue violation notices.

Proponent and exception authority. The proponent of this regulation is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include a formal

review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions and provides an internal control evaluation for use in evaluating key internal controls (see appendix D).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of the Office of the Provost Marshal General (DAPM–MPO–LE), 2800 Army Pentagon, Washington, DC 20310–2800.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Provost Marshal General (DAPM–MPO–LE), 2800 Army Pentagon, Washington, DC 20310–2800.

Committee management. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527. Further, if it is determined that an established “group” identified within this regulation, later takes on the characteristics of a committee, as found in

*This regulation supersedes AR 190–45, dated 30 March 2007, and AD 2013–06, dated 14 February 2013.

the AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1–1, *page 1*

References • 1–2, *page 1*

Explanation of abbreviations and terms • 1–3, *page 1*

Responsibilities • 1–4, *page 1*

Chapter 2

Records Administration, page 19

General • 2–1, *page 19*

Safeguarding official information • 2–2, *page 20*

Special requirements of The Privacy Act of 1974 • 2–3, *page 20*

Administration of expelled or barred persons file • 2–4, *page 20*

Police intelligence and criminal information • 2–5, *page 21*

Name checks • 2–6, *page 21*

Registration of sex offenders on Army installations (inside and outside the continental United States) • 2–7, *page 22*

Collection of deoxyribonucleic acid • 2–8, *page 23*

Armed escorts and unique Federal agency number documentation • 2–9, *page 25*

Chapter 3

Release of Information, page 25

General • 3–1, *page 25*

Guidelines for disclosure within the Department of Defense • 3–2, *page 26*

Release of information • 3–3, *page 26*

Release of information under the Freedom of Information Act • 3–4, *page 26*

Release of information under The Privacy Act of 1974 • 3–5, *page 27*

Amendment of records • 3–6, *page 27*

Accounting for military police record disclosure • 3–7, *page 28*

Release of law enforcement information furnished by foreign governments or international organizations • 3–8, *page 28*

Release of domestic incidents reports to the Army Family Advocacy Program • 3–9, *page 28*

Chapter 4

Offense Reporting, page 28

General • 4–1, *page 28*

Law Enforcement Report • 4–2, *page 28*

Identifying criminal incidents and subjects of investigation • 4–3, *page 29*

Offense codes • 4–4, *page 30*

Military police codes • 4–5, *page 30*

Reserve component, U.S. Army Reserve, and Army National Guard personnel • 4–6, *page 30*

DA Form 4833 (Commander's Report of Disciplinary or Administrative Action) • 4–7, *page 30*

Contents—Continued

- Updating DA Form 190–45–SG (Army Law Enforcement Reporting and Tracking System (ALERTS)) • 4–8, *page 32*
- FBI Form R–84 and final disposition report submission requirements • 4–9, *page 32*
- Procedures for reporting absence without leave, desertion, and special category absentee offenses • 4–10, *page 35*
- Vehicle Registration System • 4–11, *page 36*
- Establishing memorandums of understanding • 4–12, *page 36*
- Lost, abandoned, or unclaimed property • 4–13, *page 37*
- Procedures for restricted and unrestricted reporting in sexual assault cases • 4–14, *page 38*
- Procedures for restricted and unrestricted reporting in domestic violence cases • 4–15, *page 38*
- Domestic violence • 4–16, *page 39*
- Protection orders • 4–17, *page 39*
- Defense Incident-Based Reporting System/National Incident-Based Reporting System reporting responsibilities • 4–18, *page 39*

Chapter 5

Army Law Enforcement Trends and Analysis Report, *page 40*

- General • 5–1, *page 40*
- Crime rate reporting • 5–2, *page 41*

Chapter 6

Victim and Witness Assistance Procedures, *page 41*

- General • 6–1, *page 41*
- Procedures • 6–2, *page 41*
- Notification • 6–3, *page 42*
- Statistical reporting requirements • 6–4, *page 42*

Chapter 7

Related Military Police Forms, *page 42*

- General • 7–1, *page 42*
- DD Form 460 (Provisional Pass) • 7–2, *page 42*
- DD Form 553 (Deserter/Absentee Wanted by the Armed Forces) • 7–3, *page 42*
- DD Form 616 (Report of Return of Absentee) • 7–4, *page 43*
- DD Form 2708 (Receipt for Pre Trial/Post Trial Prisoner or Detained Person) • 7–5, *page 43*
- DD Form 1408 (Armed Forces Traffic Ticket) • 7–6, *page 43*
- United States District Court Central Violations Bureau Form • 7–7, *page 43*
- DD Form 1920 (Alcohol Incident Report) • 7–8, *page 44*
- DA Form 2804 (Crime Records Data Reference) • 7–9, *page 44*
- DA Form 2823 (Sworn Statement) • 7–10, *page 44*
- DA Form 3881 (Rights Warning Procedure/Waiver Certificate) • 7–11, *page 44*
- DA Form 3626 (Vehicle Registration/Driver Record) • 7–12, *page 44*
- DA Form 3945 (Military Police Radio Log) • 7–13, *page 44*
- DA Form 3946 (Military Police Traffic Accident Report) • 7–14, *page 44*
- The blotter report • 7–15, *page 45*
- DA Form 4002 (Evidence/Property Tag) • 7–16, *page 45*
- DA Form 4137 (Evidence/Property Custody Document) • 7–17, *page 45*
- Accountability of DD Form 1408 and the Central Violations Bureau Form • 7–18, *page 45*

Chapter 8

Reportable Serious Incidents, *page 46*

- Policy • 8–1, *page 46*
- Category 1 reportable serious incidents • 8–2, *page 46*
- Category 2 reportable serious incidents • 8–3, *page 47*
- Category 3 reporting criteria • 8–4, *page 49*
- Operational reporting reports • 8–5, *page 49*
- Incidents reportable by means other than serious-incident reports • 8–6, *page 49*

Contents—Continued

Suspicious activity report • 8–7, *page 49*

Chapter 9

Reporting Procedures for Serious-Incident Reports, *page 51*

Special handling of reports • 9–1, *page 51*

Time requirements and means of reporting • 9–2, *page 51*

Types of serious-incident reports and reporting formats • 9–3, *page 53*

Protected identity • 9–4, *page 56*

Reporting incidents when reporting responsibility is transferred • 9–5, *page 56*

Required information addressees on serious-incident reports • 9–6, *page 56*

Chapter 10

U.S. Magistrate Court, *page 56*

Relationship to Army • 10–1, *page 56*

U.S. Magistrate Court objectives • 10–2, *page 56*

Court appearances • 10–3, *page 56*

Central Violations Bureau • 10–4, *page 57*

Chapter 11

Use of United States District Court Central Violations Bureau Form, *page 57*

General • 11–1, *page 57*

Important guidelines for issuing the U.S. District Court Central Violations Bureau Form • 11–2, *page 58*

Issue and disposition procedures • 11–3, *page 58*

Fines, collateral, and nonpayment delinquencies • 11–4, *page 58*

Notification to commanders and supervisors • 11–5, *page 58*

Use of statement of probable cause • 11–6, *page 58*

Mandatory appearance • 11–7, *page 59*

Submitting mandatory hearing violations • 11–8, *page 59*

Submitting forms to the Central Violations Bureau • 11–9, *page 59*

Agency requests to dismiss or void a Central Violations Bureau form • 11–10, *page 59*

Request for dismissal or void by the defendant • 11–11, *page 59*

Central Violations Bureau Forms issued to unattended vehicles • 11–12, *page 60*

U.S. magistrate judge docket report • 11–13, *page 60*

Request to agency for a better address • 11–14, *page 60*

Undeliverable warning letters referred to U.S. magistrate judge • 11–15, *page 60*

Notice to appear letters • 11–16, *page 60*

Warrant • 11–17, *page 60*

Suspension notices • 11–18, *page 61*

Agency notification • 11–19, *page 61*

Hearing types • 11–20, *page 61*

Forfeiture of collateral on a court docket • 11–21, *page 61*

Payment by credit card • 11–22, *page 61*

Payroll deductions • 11–23, *page 61*

Citations on the docket to be reset • 11–24, *page 61*

Agency monthly reports • 11–25, *page 61*

Waiver of venue for plea and sentence • 11–26, *page 61*

Intra-district transfer • 11–27, *page 62*

Voice Case Information System • 11–28, *page 62*

Central Violations Bureau database search option through email • 11–29, *page 62*

Disposition of personnel subject to the Uniform Code of Military Justice • 11–30, *page 62*

Disposition of juvenile offenders • 11–31, *page 62*

Chapter 12

National Crime Information Center Policy, *page 63*

Authority • 12–1, *page 63*

Contents—Continued

Standards • 12-2, *page 63*

Authorized access • 12-3, *page 63*

Reports of positive urinalysis-test results entered into the National Instant Checks System database through National Crime Information Center • 12-4, *page 63*

Chapter 13

National Crime Information Center Procedures, *page 64*

Requesting an originating agency identifier • 13-1, *page 64*

Suspension or revocation • 13-2, *page 65*

Entry • 13-3, *page 65*

Modification • 13-4, *page 67*

Cancellation • 13-5, *page 67*

Validation • 13-6, *page 67*

Army participation in Criminal Justice Information System • 13-7, *page 67*

Appendixes

A. References, *page 68*

B. Contact information and mailing addresses for serious-incident reports, *page 78*

C. Offense codes for Army investigations, *page 80*

D. Internal Control Evaluation, *page 95*

Table List

Table 1-1: Geographical area of responsibilities, *page 4*

Table 4-1: List of offenses from the Uniform Code of Military Justice, *page 34*

Table C-1: Offense code list, *page 80*

Table C-2: Offense codes for Army investigation reports, *page 93*

Figure List

Figure 9-1: Format and instructions for preparing a serious incident report, *page 52*

Figure 9-1: Format and instructions for preparing a serious incident report, continued, *page 53*

Figure 9-2: Format for a serious incident report add-on, which is used to update an earlier report, *page 54*

Figure 9-2: Format for a serious incident report add-on, which is used to update an earlier report, continued, *page 55*

Figure 13-1: Sample request from a regional office of the Installation Management Command to obtain an originating agency identifier, *page 64*

Figure 13-2: Sample request—from an Army command, Army service component command, or direct reporting unit—to obtain an originating agency identifier, *page 65*

Figure 13-3: Sample of an originating agency identifier holder agreement, *page 66*

Glossary

Chapter 1 Introduction

1–1. Purpose

This regulation prescribes policies, procedures, and responsibilities on the preparation, reporting, use, retention, and disposition of Department of the Army (DA) forms and documents, listed in sections III and IV of appendix A, related to law enforcement (LE) activities. It implements Federal reporting requirements on serious incidents, crimes, and misdemeanor crimes. It also assigns the geographic areas of responsibility to a specific installation Provost Marshal Office (PMO) or Directorate of Emergency Services (DES).

1–2. References

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Responsibilities

a. Provost Marshal General. The PMG will—

(1) Establish and develop policy and procedures for the following:

(a) Preparation, use, and disposition of military police (MP) records and forms listed in sections III and IV of appendix A.

(b) Army participation in the Criminal Justice Information System (CJIS), the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications Systems (NLETS), and Army access to State LE and criminal justice agency information consistent with applicable State and Federal laws.

(c) Reporting serious incidents to Headquarters, Department of the Army (HQDA).

(2) Maintain the official record of serious-incident reports (SIRs) submitted to HQDA. All official records will be maintained in accordance with AR 25–400–2.

(3) Report crime within the Army, develop Armywide crime statistics, and coordinate LE reporting to the CJIS, the Federal Bureau of Investigation (FBI), and the Department of Justice (DOJ).

(4) Establish and manage the DA Form 190–45–SG (Army Law Enforcement Reporting and Tracking System (ALERTS)), as the automated Records Management System (RMS) within the Army. This includes procedures for entering records, retaining records, disseminating records, and using such records by DA, Department of Defense (DOD) agencies, and Federal, State, and local LE agencies.

(5) Prepare and execute the DA's agreement to use the services of NLETS and participation in CJIS.

(6) Ensure that those counterintelligence (CI) related incidents specified in AR 381–12 are properly reported to the local Army CI field office or the Army Counterintelligence Coordinating Authority at Fort Belvoir, VA.

b. Commander, Installation Management Command; Commander, U.S. Army Materiel Command; Commander, U.S. Army Medical Command; commanders of Army commands, Army service component commands, and direct reporting units—excluding the U.S. Army Criminal Investigation Command—who have reporting or oversight responsibilities under this regulation (such as the Director, Army National Guard, and Commander, Military Surface Deployment and Distribution Command). The commanders for IMCOM, AMC, MEDCOM, ACOMs, ASCCs, relevant DRUs excluding USACIDC; the Director, ARNG; and Commander, SDDC will ensure that subordinate garrison commanders—

(1) Use DA Form 190–45–SG, also known as ALERTS, to meet reporting requirements prescribed in this regulation.

(2) Appoint, in writing, a system administrator for DA Form 190–45–SG, also known as ALERTS, and ensure the system's maintenance.

(3) Comply with all referenced provisions of Federal law in this regulation.

(4) Submit required criminal history data to the U.S. Army Crime Records Center (USACRC) for transmittal to CJIS.

(5) Forward requests for participation in NCIC that meet the criteria of this regulation to the Director, U.S. Army Crime Records Center (CICR–CR), 27130 Telegraph Road, Quantico, VA 22134.

(6) Ensure that installation provost marshals (PMs) or directors of emergency services (DESs) enter into State-government user agreements for access to State LE telecommunications systems and agencies.

(7) Report serious incidents to HQDA as prescribed by this regulation.

(8) Ensure that installation PMs or DESs execute liaison coordination and information exchange with civilian LE authorities within their geographic area of responsibility.

(9) Report incidents occurring off the installation, in DA Form 190–45–SG also known as ALERTS, in the geographic areas for PM or DES activities prescribed by table 1–1.

(10) If an installation is a Joint service base, ensure commanders abide by the IMCOM-facilitated memorandum of

agreement, which addresses each Service's reporting requirement. The Army chain of command reporting requirements are still required in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.03D for operational reporting and this regulation for serious-incident reporting.

(11) Establish additional reporting categories as prescribed in paragraph 8–4, below, if desired.

(12) Appoint in writing a victim/witness coordinator. This coordinator is responsible for the LE notification requirements to all identified victims and witnesses of crime.

c. Senior commanders. These leaders will—

(1) Ensure that commanders at all levels report alleged criminal incidents to the installation PMO or Directorate of Emergency Services, and the USACIDC, for appropriate inquiry and investigation.

(2) Ensure submission of DA Form 4833 (Commander's Report of Disciplinary or Administrative Action) to their local installation PMO or DES on dispositions of cases referred to them for action by an investigating officer (commander's inquiry or AR 15–6 investigation) and those incidents outlined in paragraph 4–19 of this regulation.

(3) Ensure that battalion commanders or the first lieutenant colonel in the chain of command (of the Soldier in the "SUBJECT" block) complete and return the DA Form 4833 within 60 days with supporting documentation (copies of investigations under Article 15, Uniform Code of Military Justice; court martial orders; reprimands; and so forth) for all USACIDC investigations. Army civilian and contract personnel will also have a DA Form 4833 completed by their military supervisor with special courts martial convening authority. The unit and brigade commanders, or their equivalent, will also receive a copy of the DA Form 4833 for all USACIDC investigations.

(4) Ensure that company, troop, and battery level commanders complete and return the DA Form 4833 within 60 days with supporting documentation (copies of investigations under UCMJ, Art. 15; court martial orders; reprimands; and so on) in all cases investigated by MP investigations, civilian detectives employed by the DA, and the PMO or DES.

(5) Ensure their senior MP commanders and/or installation PMs or DESs provide to their subordinate garrisons and installations staff, oversight, and technical assistance for MP-related issues.

d. The Commanding General, U.S. Army Criminal Investigation Command. The CG, USACIDC will provide reports and/or statistical data to installation PMs or DESs in order to support commands with the relative number and types of serious crimes and incidents investigated, subjects identified, value of property stolen or recovered, and other information reflecting the status of discipline, law, and order necessary for the completion of reports required by HQDA. Statistical data necessary to support locally established reports may be provided within the administrative and record-keeping capabilities of the supporting USACIDC element.

e. The Commanding General, U.S. Army Training and Doctrine Command. The CG, TRADOC will—

(1) Ensure that technical training on DA Form 190–45–SG, also known as ALERTS, for functional users, is incorporated within the instructional programs of service schools.

(2) Ensure that the requirements of completing the DA Form 4833 are incorporated within the company through a brigade-level commanders' course.

(3) Ensure the DA Form 4833 requirements are briefed to commanders and command sergeants major during the Garrison Pre-command Course.

f. The Director, U.S. Army Crime Records Center. The Director, USACRC will—

(1) Serve as the Army's collection point and analytic center for all Army aggregate crime data.

(2) Receive the Law Enforcement Report (LER), prepared per this regulation and related Army LE regulations, policies, and procedures.

(3) Maintain records that support entries made in the FBI's CJIS. This includes the criminal history file of the NCIC.

(4) Respond to requests for information received from local, State, Federal, and international law enforcement agencies.

(5) Process amendment requests under Section 552a, Title 5, United States Code (The Privacy Act) in coordination with installation PMs and DESs.

(6) Be responsible to the PMG for coordinating installation PM or DES participation in CJIS and NCIC, and resolution of operational issues concerning the DA's participation in CJIS and NLETS.

(7) Be responsible to the Commander, USACIDC for establishing internal NCIC operating policies based on rules and operating policies of the NCIC Advisory Policy Board and State control terminal agencies (CTAs).

(8) Appoint a CJIS systems officer to represent the PMG at working group meetings for CJIS and NLETS.

(9) Enter into a user agreement with CJIS concerning the Army's adherence to all CJIS operating policies and regulations and, where applicable, State criminal justice agencies.

g. Other commanders. The MP brigade or battalion combat support commanders (who may be dual-hatted as an installation PM or DES), and the ACOM, ASCC, DRU, and installation PMs and DESs in charge of LE operations will—

(1) Provide staff oversight and technical assistance for LE-related issues to installation and garrison commanders and IMCOM regional directors. They will also provide supported commands with staff review and advice concerning

doctrine, organization, training, materiel, leadership and education, personnel and facilities, and resourcing and LE policy development.

(2) Comply with crime records and reporting requirements of this regulation and ensure that documents and forms, listed in section III of appendix A, are accurately completed and forwarded as prescribed per this regulation.

(3) Respond to routine requests for information received from local, State, Federal, international law enforcement agencies, and requests for information under Title 5, United States Code, Section 552a (The Privacy Act) and Title 5, United States Code, Section 552 (The Freedom of Information Act).

(4) Enforce all laws and regulations pertaining to misdemeanors and felonies, if declined by USACIDC.

(5) Assure adherence by Army installation LE personnel to provisions of this regulation, with the exception of changes dictated by the U.S. Magistrate or U.S. District Court of the judicial district in which their installation is located.

(6) Ensure violations issued on the Central Violations Bureau (CVB) Form (United States District Court Violation Notice) are entered into the DA Form 190–45–SG, also known as ALERTS, and closed when complete. The DD Form 1408 (Armed Forces Traffic Ticket) will be entered into the DA Form 190–45–SG, also known as ALERTS, for violations outside the continental United States (OCONUS).

(7) Ensure that release of LE information complies with 5 USC 552a (The Privacy Act), 5 USC 552 (The Freedom of Information Act), and chapter 3 of this regulation.

(8) Ensure that funding requirements for NCIC equipment, software, and maintenance are submitted through the appropriate resourcing channels.

(9) Ensure that all NCIC transactions are in compliance with this regulation, operating policies of the NCIC, and the State CTA.

(10) Ensure that NCIC terminals are staffed 24 hours per day or secured to preclude access by unauthorized personnel.

(11) Ensure that NCIC terminal operators successfully complete required training on the NCIC and State systems.

(12) Appoint an NCIC terminal coordinator in writing, identifying their duties and responsibilities.

(13) Ensure execution of NCIC inquiries for the USACIDC special agents in support of criminal investigations or related inquiries.

(14) Be responsive to the Federal service coordinator and State CTA in operating the NCIC and State law enforcement telecommunications systems and for access to, and dissemination of, criminal information. (Note: OCONUS exempt from NCIC requirements throughout this regulation.)

(15) Ensure execution of necessary liaison and coordination with civilian authorities, within their geographic area of responsibility. For details on these assignments, see table 1–1.

(16) Upon apprehension or initiation of investigation of a Soldier, DOD civilian, or contractor, by installation or civilian LE officer immediately notify (within 4 hours) the chain of command (commander, deputy director, or civilian equivalent) and document via the LER. (Exception for semi-covert investigations in which notification could compromise the integrity or successful resolution of investigations, in these cases, only if the subject is notified that he or she is under investigation, then the commander will also be informed of the investigation).

(17) Release Soldiers under law enforcement control only to the commander, command sergeant major, or first sergeant via DD Form 2708 (Receipt for Pre Trial/Post Trial Prisoner or Detained Person).

(18) Ensure accountability for all Soldiers and prisoners confined in local civilian confinement facilities using the Army Corrections Information System module of DA Form 190-45-SG, also known as ALERTS. AR 190–47 authorizes installations without an Army corrections facility to contract the incarceration of Army pretrial prisoners in Federally approved local civilian jails, when military facilities are not available and prisoners are sentenced to confinement locally for 30 or fewer days. Copies of agreements will be forwarded to the Army Corrections Command for review and recommendation. See AR 190–47 for other confinement policy and procedures.

(19) Screen all LERs for possible alcohol or other drug abuse involvement, and provide the Army Substance Abuse Program (ASAP) manager with excerpts from the blotter report on all incidents involving alcohol, drugs, or other substance abuse on a daily basis.

(20) Request the assistance of civilian local and State law enforcement agencies, upon request from a reserve component commander, to determine the whereabouts and welfare of USAR Soldiers when a second unexcused absence from a unit training assembly occurs.

h. Directors of Emergency Services. Each Director of Emergency Services, for installations and for regions, is responsible for maintaining the DA Form 190–45–SG, also known as ALERTS. The system administrators for the DA Form 190–45–SG are appointed, in writing, by the installation.

i. Victim/witness coordinator. The victim/witness coordinator, who is appointed in writing by the installation PMO or DES, is responsible for fulfilling the LE notification requirements to all identified victims and witnesses of crime.

j. U.S. Army Reserve commanders. All U.S. Army Reserve (USAR) commanders unit, agency, or activity commanders will submit SIRs thru the Army Reserve Watch, then follow the steps in paragraph *k*, below.

k. Commanders of active, unified, or combined command elements. All active Army and USAR unit, agency, or activity commanders, to include commanders of Army elements of unified or combined commands, will—

(1) Notify the continental United States (CONUS) installation commander having geographic reporting responsibility or the overseas ASCC commander and the appropriate region DES, as appropriate, of serious incidents immediately.

(2) Provide follow up information for supplementary reporting, as necessary.

(3) The ARNGUS reports will include the State Adjutant General Office and the National Guard Bureau as information addressees.

(4) In accordance with AD 2011-17, dated 21 September 2011, all U.S. Army commissioned officers, warrant officers, and enlisted members above the pay grade of E-6, who are on active duty or in an active status in the reserve component, will report in writing via DA Form 4187 (Personnel Action), any conviction of such member for violation of a criminal law of the United States—whether or not the member is on active duty or in an active status at the time of the conduct that provides the basis for the conviction.

l. Commanders of installations within the continental United States. The commanders of CONUS installations may transfer reporting responsibility to another CONUS installation commander by mutual agreement, subject to PMG approval. Transfer procedures are described in paragraph 9-5 of this regulation.

m. Director, U.S. Army Criminal Investigation Laboratory. The Director, USACIL will—

(1) Be responsible to the PMG for guidance identifying live-scan, electronic, fingerprint and palm-print equipment that is compatible with the FBI’s electronic fingerprint transmission specification and electronic biometric transmission standard, the American National Standards Institute, the National Institute of Standards and Technology, national LE standards for fingerprints or palm prints, and USACIL’s Automated Fingerprint Identification System.

(2) Be responsible for all USACIL Integrated Automated Fingerprint Identification System (IAFIS) transactions involving latent finger and palm prints.

(3) Be responsible for Army LE coordination with the FBI concerning IAFIS databases to include the criminal master file, civil files, and special latent cognizant files.

(4) Enter into a user agreement with CJIS concerning the USACIL’s adherence to all CJIS operating policies and regulations involving latent print transactions and IAFIS files.

(5) Enter into a user agreement with CJIS concerning the Army’s adherence to all CJIS operating policies and regulations involving latent print transactions and special latent cognizant files.

n. National Crime Information Center terminal coordinator. The NCIC terminal coordinator will—

(1) Ensure the accuracy of entries and validating records.

(2) Respond to inquiries.

(3) Ensure physical security of the terminal.

o. National Crime Information Center terminal coordinator at the U.S. Army Deserter Information Point. The NCIC terminal coordinator at the U.S. Army Deserter Information Point (USADIP) will be responsible for—

(1) The NCIC entries concerning U.S. Army deserters.

(2) The NCIC terminal operations at the Personnel Control Facility, Fort Knox, KY.

(3) Criminal-history record checks for identifying and verifying Army deserters, parole violators, and escaped prisoners.

(4) The NCIC records of parole violators and escaped military prisoners.

p. Installation staff judge advocates. SJAs will advise Army installation commanders and installation PMs, DESs, or security officers concerning implementation of this regulation as requested.

Table 1-1
Geographical area of responsibilities

Installation	Area of responsibility
Aberdeen Proving Ground	a. Delaware county (1) New Castle b. Maryland counties (1) Baltimore (2) Cecil (3) Harford (4) Kent c. New Jersey counties (1) Atlantic (2) Camden (3) Cape May (4) Cumberland (5) Gloucester

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
	(6) Salem d. Pennsylvania counties (1) Berks (2) Bucks (3) Chester (4) Delaware (5) Lancaster (6) Lebanon (7) Lehigh (8) Montgomery (9) Northampton (10) Philadelphia
Fort AP Hill, VA	a. Virginia counties (1) Caroline (2) Essex (3) Hanover (4) King and Queen (5) King George (6) King William (7) Lancaster (8) Louisa (9) Northumberland (10) Richmond (11) Spotsylvania (12) Westmoreland b. West Virginia counties (1) Boone (2) Clay (3) Fayette (4) Greenbrier (5) Jackson (6) Kanawha (7) Lincoln (8) Logan (9) McDowell (10) Mercer (11) Monroe (12) Nicholas (13) Putman (14) Raleigh (15) Roane (16) Summers (16) Wyoming
Fort Belvoir, VA	a. Virginia counties (1) Albemarle (2) Augusta (3) Bath (4) Clarke (5) Culpeper (6) Fauquier (7) Frederick (8) Greene (9) Highland (10) Madison (11) Orange (12) Page (13) Rappahannock (14) Rockingham (15) Shenandoah (16) Stafford (17) Warren b. West Virginia counties (1) Barbour (2) Berkeley (3) Braxton (4) Brooke (5) Calhoun (6) Dodd-Ridge (7) Gilmer (8) Grant

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
	(9) Hampshire (10) Hancock (11) Hardy (12) Harrison (13) Jefferson (14) Lewis (15) Marion (16) Marshall (17) Mineral (18) Monongalia (19) Morgan (20) Ohio (21) Pendleton (22) Pleasants (23) Pocahontas (24) Preston (25) Randolph (26) Ritchie (27) Taylor (28) Tucker (29) Tyler (30) Upshur (31) Webster (32) Wetzel (33) Wirt (34) Wood
Fort Benning, GA	a. Florida counties (1) Bay (2) Calhoun (3) Columbia (4) Dixie (5) Escambia (6) Franklin (7) Gadsden (8) Gilchrist (9) Gulf (10) Hamilton (12) Jackson (11) Holmes (13) Jefferson (14) Lafayette (15) Leon (16) Liberty (17) Madison (18) Okaloosa (19) Santa Rosa (20) Suwannee (21) Taylor (22) Wakulla (23) Walton (24) Washington b. Georgia counties (1) Baker (2) Bartow (3) Berrien (4) Bleckley (5) Calhoun (6) Carroll (7) Chattahoochee (8) Cherokee (9) Clay (10) Clayton (11) Cobb (12) Colquitt (13) Columbus-Muscogee (14) Cook (15) Coweta (16) Crawford (17) Crisp (18) Decatur

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
	<ul style="list-style-type: none"> (19) Dooly (20) Dougherty (21) Douglas (22) Early (23) Fayette (24) Fulton (25) Grady (26) Haralson (27) Harris (28) Heard (29) Houston (30) Lamar (31) Lee (32) Macon (33) Marion (34) Meriwether (35) Miller (36) Mitchell (37) Monroe (38) Paulding (39) Peach (40) Pickens (41) Pike (42) Pulaski (43) Quitman (44) Randolph (45) Schley (46) Seminole (47) Spalding (48) Stewart (49) Sumter (50) Talbot (51) Taylor (52) Terrell (53) Thomas (54) Tift (55) Troup (56) Turner (57) Upson (58) Webster (59) Wilcox (60) Worth c. Alabama counties (1) Chambers (2) Lee (3) Russell
Fort Bliss, TX	<ul style="list-style-type: none"> a. All New Mexico counties, except (1) Catron (2) Grant (3) Hidalgo b. All Texas counties west of, and including (1) Bailey (2) Crockett (3) Dawson (3) Hockley (4) Lubbock (5) Lynn (6) Martin (7) Midland (8) Pecos (9) Terrell (10) Upton (11) Val Verde

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
Fort Bragg, NC	a. All North Carolina counties b. Tennessee counties (1) Carter (2) Johnson (3) Sullivan (4) Unicoi (5) Washington c. Virginia counties (1) Bland (2) Buchanan (3) Carroll (4) Dickenson (5) Floyd (6) Grayson (7) Henry (8) Lee (9) Patrick (10) Pulaski (11) Russell (12) Scott (13) Smyth (14) Tazewell (15) Washington (16) Wise (17) Wythe
Fort Buchanan, PR	a. All of Puerto Rico b. U.S. Virgin Islands
Fort Campbell, KY	a. Arkansas counties (1) Crittenden (2) Lee (3) Mississippi (4) Monroe (5) Phillips (6) St. Francis b. All Illinois counties east and south of, and including (1) Clark (2) Cumberland (3) Fayette (4) Franklin (5) Jackson (6) Jefferson (7) Marion (8) Shelby c. All Kentucky counties west of, and including (1) Allen (2) Butler (3) Daviess (4) Ohio (5) Warren d. All Mississippi counties north of, and including (1) Clay (2) Coahoma (3) Grenada (4) Monroe (5) Tallahatchie (6) Webster e. All Tennessee counties not listed under Fort Bragg, Fort Knox, and Redstone Arsenal
Carlisle Barracks, PA	a. All Ohio counties east of, and including (1) Coshocton (2) Guernsey (3) Holmes (4) Lorain (5) Medina (6) Monroe (7) Noble (8) Wayne b. All Pennsylvania counties not listed under Aberdeen Proving Ground

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
Fort Carson, CO	a. All Colorado counties b. All Montana counties east of, and including (1) Fergus (2) Park (3) Phillips (4) Sweet Grass (5) Wheatland c. All Nebraska counties west of, and including (1) Arthur (2) Grant (3) Hayes (4) Hitchcock (5) Keith (6) Perkins (7) Sheridan d. All Utah counties e. All Wyoming counties
Fort Detrick, MD	Maryland counties (1) Allegany (2) Carroll (3) Frederick (4) Garrett (5) Washington
Fort Drum, NY	a. All New York counties except those listed under Fort Hamilton b. All Maine counties c. All Massachusetts counties d. All New Hampshire counties e. All Vermont counties

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
Fort Gordon, GA	Georgia counties (1) Baldwin (2) Banks (3) Barrow (4) Bibb (5) Bulloch (6) Burke (7) Butts (8) Candler (9) Clarke (10) Columbia (11) Dawson (12) DeKalb (13) Elbert (14) Emanuel (15) Forsyth (16) Franklin (17) Glascock (18) Greene (19) Gwinnett (20) Habersham (21) Hall (22) Hancock (23) Hart (24) Henry (25) Jackson (26) Jasper (27) Jefferson (28) Jenkins (29) Johnson (30) Jones (31) Laurens (32) Lincoln (33) Lumpkin (34) Madison (35) McDuffie (36) Montgomery (37) Morgan (38) Newton (39) Oconee (40) Oglethorpe (41) Putnam (42) Rabun (43) Richmond (44) Rockdale (45) Screven (46) Stephens (47) Taliaferro (48) Towns (49) Treutlen (50) Twiggs (51) Union (52) Walton (53) Warren (54) Washington (55) Wheeler (56) White (57) Wilkes (58) Wilkinson f. All Rhode Island counties g. All Vermont counties
Fort Hamilton, NY	a. All Connecticut counties b. All New York counties south of, and including (1) Columbia (2) Greene (3) Sullivan (4) Ulster c. All New Jersey counties except those listed under Aberdeen Proving Ground d. All Rhode Island counties

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
Fort Hood, TX	a. All Texas counties south, and east, of (1) Cottle (2) Crockett (3) Dawson (4) Floyd (5) Foard (6) Hale (7) Lamb (8) Lubbock (9) Lynn (10) Martin (11) Midland (12) Motley (13) Upton (14) Wichita (15) Wilbarger (16) Val Verde
Fort Huachuca, AZ	a. All Arizona counties b. New Mexico counties (1) Catron (2) Grant (3) Hidalgo
Fort Irwin, CA	a. All California counties not listed under Fort Lewis b. All Nevada counties
Fort Jackson, SC	a. All South Carolina counties, except (1) Beaufort (2) Jasper b. Tennessee counties (1) Coker (2) Greene

**Table 1-1
Geographical area of responsibilities—Continued**

Installation	Area of responsibility
Fort Knox, KY	<ul style="list-style-type: none"> a. All Illinois counties east and north of, and including <ul style="list-style-type: none"> (1) Boone (2) Coles (3) De Kalb (4) DeWitt (5) Edgar (6) LaSalle (7) Livingston (8) Macon (9) McLean (10) Moultrie b. All Indiana counties c. All Kentucky counties east of <ul style="list-style-type: none"> (1) Allen (2) Butler (3) Daviess (4) Ohio (5) Warren d. All Michigan counties e. All Ohio counties west of <ul style="list-style-type: none"> (1) Coshocton (2) Guernsey (3) Holmes (4) Lorain (5) Medina (6) Monroe (7) Noble (8) Wayne f. Tennessee counties <ul style="list-style-type: none"> (1) Campbell (2) Claiborne (3) Clay (4) Fentress (5) Hancock (6) Hawkins (7) Jackson (8) Morgan (9) Overton (10) Pickett (11) Scott g. West Virginia counties <ul style="list-style-type: none"> (1) Cabell (2) Mason (3) Mingo (4) Wayne
Fort Leavenworth, KS	<ul style="list-style-type: none"> a. All Iowa counties b. All Kansas counties east of, and including <ul style="list-style-type: none"> (1) Brown (2) Coffey (3) Jackson (4) Montgomery (5) Osage (6) Shawnee (7) Wilson (8) Woodson c. All Minnesota counties d. All Wisconsin counties

**Table 1-1
Geographical area of responsibilities—Continued**

Installation	Area of responsibility
Fort Lee, VA	Virginia counties (1) Accomack (2) Alleghany (3) Amelia (4) Amherst (5) Appomattox (6) Bedford (7) Botetourt (8) Brunswick (9) Buckingham (10) Campbell (11) Charles City (12) Charlotte (13) Chesapeake City (14) Chesterfield (15) Colonial Heights (16) Craig (17) Cumberland (18) Dinwiddie (19) Franklin (20) Fluvanna (21) Giles (22) Gloucester (23) Goochland (24) Greensville (25) Halifax (26) Hampton Cities (27) Henrico (28) Hopewell (29) Isle of Wight (30) James City (31) Lunenburg (32) Mathews (33) Mecklenburg (34) Middlesex (35) Montgomery (36) Nelson (37) New Kent (38) Newport News (39) Norfolk City (40) Northampton (41) Nottoway (42) Petersburg (43) Pittsylvania (44) Portsmouth City (45) Powhatan (46) Prince Edward (47) Prince George (48) Roanoke (49) Rockbridge (50) Southampton (51) Suffolk City (52) Surry (53) Sussex (54) Virginia Beach City (55) York
Fort Leonard Wood, MO	a. All Arkansas counties not listed under Fort Campbell, Fort Polk, and Fort Sill b. All Illinois counties not listed under Fort Campbell and Fort Knox c. All Missouri counties

**Table 1-1
Geographical area of responsibilities—Continued**

Installation	Area of responsibility
Fort Lewis, WA	<ul style="list-style-type: none"> a. California counties <ul style="list-style-type: none"> (1) Del Norte (2) Humboldt (3) Modoc (4) Shasta (5) Siskiyou (6) Trinity b. All Idaho counties c. All Montana counties west of <ul style="list-style-type: none"> (1) Fergus (2) Park (3) Phillips (4) Sweet Grass (5) Wheatland d. All Oregon counties e. All Washington counties
Fort Meade, MD	<ul style="list-style-type: none"> a. All Maryland counties not listed under Fort Myer, Fort Detrick, and Aberdeen Proving Ground b. Delaware counties <ul style="list-style-type: none"> (1) Kent (2) Sussex
Fort Myer, VA	<ul style="list-style-type: none"> a. All of District of Columbia b. Maryland counties <ul style="list-style-type: none"> (1) Montgomery (2) Prince George's c. Virginia cities <ul style="list-style-type: none"> (1) Alexandria (2) Fairfax (3) Manassas (4) Manassas Park d. Virginia counties <ul style="list-style-type: none"> (1) Arlington (2) Fairfax (3) Loudoun (4) Prince William
Fort Polk, LA	<ul style="list-style-type: none"> a. All Arkansas counties south of, and including <ul style="list-style-type: none"> (1) Arkansas (2) Desha (3) Garland (4) Grant (5) Jefferson (6) Montgomery (7) Polk (8) Saline b. All Louisiana parishes c. All Mississippi counties west and south of, and including <ul style="list-style-type: none"> (1) Attala (2) Bolivar (3) Carroll (4) Jefferson Davis (5) Leake (6) Leflore (7) Marion (8) Montgomery (9) Rankin (10) Simpson (11) Sunflower

**Table 1-1
Geographical area of responsibilities—Continued**

Installation	Area of responsibility
Redstone Arsenal	<ul style="list-style-type: none"> a. All Alabama counties except those listed under Fort Rucker b. Georgia counties <ul style="list-style-type: none"> (1) Catoosa (2) Chattooga (3) Dade (4) Fannin (5) Floyd (6) Gilmer (7) Gordon (8) Murray (9) Polk (10) Walker (11) Whitfield c. Tennessee counties <ul style="list-style-type: none"> (1) Anderson (2) Bledsoe (3) Blount (4) Bradley (5) Grainger (6) Hamblen (7) Hamilton (8) Jefferson (9) Knox (10) Loudon (11) Marion (12) McMinn (13) Meigs (14) Monroe (15) Polk (16) Rhea (17) Sequatchie (18) Sevier (19) Union
Fort Riley, KS	<ul style="list-style-type: none"> a. All Kansas counties not listed under Fort Leavenworth b. All Nebraska counties east of <ul style="list-style-type: none"> (1) Arthur (2) Grant (3) Hayes (4) Hitchcock (5) Keith (6) Perkins (7) Sheridan c. All North Dakota counties d. All South Dakota counties
Fort Rucker, AL	<ul style="list-style-type: none"> a. All Alabama counties south of, and including <ul style="list-style-type: none"> (1) Bibb (2) Chilton (3) Coosa (4) Greene (5) Hale (6) Sumter (7) Tallapoosa b. All Mississippi counties except those listed under Fort Campbell and Fort Polk

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
Fort Sill, OK	a. Arkansas counties (1) Crawford (2) Franklin (3) Logan (4) Scott (5) Sebastian b. All Oklahoma counties c. All Texas counties north of, and including (1) Cottle (2) Floyd (3) Foard (4) Hale (5) Lamb (6) Motley (7) Wichita (8) Wilbarger

**Table 1-1
Geographical area of responsibilities—Continued**

Installation	Area of responsibility
Fort Stewart, GA	a. All Florida counties except (1) Bay (2) Calhoun (3) Columbia (4) Dixie (5) Escambia (6) Franklin (7) Gadsden (8) Gilchrist (9) Gulf (10) Hamilton (11) Holmes (12) Jackson (13) Jefferson (14) Lafayette (15) Leon (16) Liberty (17) Madison (18) Okaloosa (19) Santa Rosa (20) Suwannee (21) Taylor (22) Wakulla (23) Walton (24) Washington b. Georgia counties (1) Appling (2) Atkinson (3) Bacon (4) Ben Hill (5) Brantley (6) Brooks (7) Bryan (8) Camden (9) Charlton (10) Chatham (11) Clinch (12) Coffee (13) DODge (14) Effingham (15) Echols (16) Evans (17) Glynn (18) Irwin (19) Jeff Davis (20) Lanier (21) Liberty (22) Long (23) Lowndes (24) McIntosh (25) Pierce (26) Tattnall (27) Telfair (28) Toombs (29) Ware (30) Wayne c. South Carolina counties (1) Beaufort (2) Jasper
USAREUR/IMCOM EUROPE	All of Europe
USARPAC/IMCOM PACIFIC	a. All of Alaska b. All of Hawaii c. All of Japan
USAG—Red Cloud	Area I
USAG—Yongsan	Area II
USAG—Humphreys	Area III

Table 1-1
Geographical area of responsibilities—Continued

Installation	Area of responsibility
USAG–Daegu	Area IV

Chapter 2 Records Administration

2-1. General

a. The MP records and files created under provisions of this regulation will be maintained and disposed of in accordance with instructions and standards prescribed by AR 25-400-2, AR 25-55, AR 340-21, AR 25-1, AR 600-63, DA Pam 600-24, and other applicable HQDA directives.

b. Each installation PM or DES will appoint, in writing, two staff members (one primary and one alternate) to account for and safeguard all records containing personally identifiable information (PII) protected by law. Action will be taken to ensure that protected personal information is used and stored only where facilities and conditions will preclude unauthorized or unintentional disclosure.

c. PII is information so unique to an individual that it enables others to identify the individual without his or her knowledge or permission; the information may be used to obtain improper financial benefit. Some examples include Social Security number (SSN), age, military rank or civilian grade, marital status, race, salary, home or office phone numbers, and other demographic, biometric, personnel, medical, or financial information.

d. The system administrators for DA Form 190-45-SG, also known as ALERTS, will have a final secret clearance. An interim secret security clearance is acceptable, provided the requisite personnel security investigation has been submitted. All users of DA Form 190-45-SG, also known as ALERTS, will undergo mandatory pre-employment background screening to make a determination as to the users' character and trustworthiness. Foreign national personnel employed by the installation PM or DES will undergo host nation LE and security agency checks, at local and national levels, where permissible by host nation law. Access to the information in DA Form 190-45-SG, also known as ALERTS, will be limited to levels no lower than installation ACOMs and ASCCs with a PM or DES.

e. Access to areas in which MP records are prepared, processed, and stored will be restricted to those personnel whose duties require their presence and to other personnel on official business. The MP records containing PII will be stored in a locked room or locked filing cabinet when not under the personal control of authorized personnel. Alternate storage systems providing equal or greater protection will be used in accordance with AR 25-55.

f. All information contained within DA Form 190-45-SG, also known as ALERTS, is restricted by law (5 USC 552a (The Privacy Act)) to those who are authorized to handle criminal justice information. In order to maintain the integrity of this sensitive information it will be accorded proper management and security, and will only be handled by personnel who have been back grounded for law enforcement work (such as LE personnel CID, MP, DACP, police administrators working for DES/PMO) and who have been trained in the appropriate handling of such sensitive information as required by State and Federal law. Activity associated with any aspect of DA Form 190-45-SG, also known as ALERTS, is subject to detailed monitoring and audits of all activity to protect against improper or unauthorized use, access or dissemination of "sensitive information." Unauthorized use, which includes requests, dissemination, sharing, copying or receipt of information within DA Form 190-45-SG, also known as ALERTS, could result in civil proceedings against the offending agency and/or criminal proceedings against any user or other person involved. Violations or misuse may also subject the user and the user's command to administrative sanctions and possible disciplinary action by their command, subject to due process, against its employee(s). This could result in termination of access to DA Form 190-45-SG, also known as ALERTS.

g. Only personnel on official business can have access to areas in which computers are used to store, process, or retrieve MP records (for example, remote computer terminals and authorized personal computers used for Government business and activities). When processing MP information, computer video display monitors will be positioned so that protected information cannot be viewed by unauthorized persons. Computer output from automated MP systems will be controlled as specified in *d* and *e*, above.

h. Output from any locally prepared data or automated systems containing personal information subject to 5 USC 552a (The Privacy Act) will be controlled in accordance with AR 340-21. All locally created unique automated systems of records containing LE information developed by ACOMs, ASCCs, DRUs, supported or supporting commands, must be reported to and approved by the PMG. The request must clearly document why DA Form 190-45-SG, also known as ALERTS, cannot meet the requirements or objectives of the organization. After review and approval by HQDA, the installation, IMCOM, USAMC, MEDCOM, and other ACOMs, ASCCs, and DRUs will complete and process the systems notice for publication in the Federal Register in accordance with AR 340-21 and 5 USC 552a (The Privacy Act).

i. The installation PMs or DESs using automated systems will appoint, in writing, as an additional duty, an information assurance security officer who will ensure implementation of automation security requirements within the organization. Passwords used to control systems access will be generated, issued, and controlled by the information assurance security officer.

j. Supervisors at all levels will ensure that personnel whose duties involve preparation, processing, filing, and release of MP records are knowledgeable of, and comply with policies and procedures contained in, this regulation, AR 25-55, AR 340-21, and other applicable HQDA directives. Particular attention will be directed to provisions on the release of information and protection of privacy.

k. The MP records identifying juveniles as offenders will be clearly marked as juvenile records and will be kept secure from unauthorized access by individuals. Juvenile records will be stored with adult records, but clearly designated as juvenile records even after the individual becomes of legal age. In distributing information on juveniles, the installation Freedom of Information Act (FOIA) Office will ensure that only individuals with a clear reason to know the identity of a juvenile are provided the PII on the juvenile. For example, a community commander is authorized to receive pertinent information on juveniles under their jurisdiction. When the LER identifying juvenile offenders must be provided to multiple commanders or supervisors, the installation FOIA Office must sanitize reports to withhold juvenile information not pertaining to that commander's area of responsibility.

l. The MP records in the custody of USACRC will be processed, stored, and maintained in accordance with policy established by the Director, USACRC.

2-2. Safeguarding official information

a. The MP records are unclassified except when they contain national security information as defined in AR 380-5.

b. When MP records containing PII are transmitted outside the installation LE community to other departments and agencies within DOD, such records will be marked "For Official Use Only" (FOUO). These records will be transmitted as prescribed by AR 25-55. Use of an expanded marking is required for certain records transmitted outside DOD per AR 25-55.

c. The MP records will also be released to Federal, State, local, or foreign LE agencies as prescribed by AR 340-21. Expanded markings will be applied to these records.

2-3. Special requirements of The Privacy Act of 1974

a. Certain PII is protected under 5 USC 552a (The Privacy Act) and AR 340-21.

b. Pursuant to 5 USC 552a(e)(3), when an Army activity asks an individual for his or her PII that will be maintained in a system of records, the activity must provide the individual with a Privacy Act Statement. A Privacy Act Statement notifies individuals of the authority, purpose, and use of the collection, whether the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.

c. Army LE personnel performing official duties often require an individual's PII, including SSN for identification purposes. This PII can be used to complete the LER and records. In addition to Executive Order 9397, as amended by EO 13478, the solicitation of the SSN is authorized by paragraph 2.c.(2) of DODI 1000.30, which covers reduction of SSN use within DOD. The purpose is to provide commanders and law enforcement officials with means by which information may accurately be identified. The SSN is used as an additional or alternate means of identification to facilitate filing and retrieval. The following procedures will be used for identification:

(1) Active Army, USAR, ARNG/ARNGUS, and retired military personnel are required to produce their common access card, or other Government-issued identification, as appropriate.

(2) Family members of sponsors will be requested to produce their DD Form 1173 (Uniformed Services Identification and Privilege Card). Information contained thereon (for example, the sponsor's SSN) will be used to verify and complete applicable sections of the LER and related forms listed in sections III and IV of appendix A.

(3) All DOD civilian personnel will be requested to produce their appropriate service identification. The DA Form 1602 (Civilian Identification) or the common access card will be requested from DA civilian employees. If unable to produce such identification, DOD civilians will be requested to provide other verifying documentation.

(4) Non-DOD civilians, including military Family members and those whose status is unknown, will be advised of the provisions of The Privacy Act Statement when requested to disclose their PII, including SSN, as required.

d. Requests for new systems of MP records, changes to existing systems, and continuation systems not addressed in existing public notices will be processed as prescribed in AR 340-21, after approval is granted by HQDA, OPMG (DAPM-MPO-LE), 2800 Army Pentagon, Washington, DC 20310-2800.

e. The statutes 5 USC 552a (The Privacy Act), 10 USC 301, and 5 USC 2951 require that Federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. Authority for soliciting SSNs is Executive Order 13478. The purpose is to provide commanders and law enforcement officials with means by which information may accurately be identified. The SSN is used as an additional or alternate means of identification to facilitate filing and retrieval. Disclosure of SSNs is voluntary.

f. Notwithstanding the requirement to furnish an individual with a PAS when his or her PII will be maintained in a system of records, AR 340-21, which covers The Army Privacy Program, provides that records contained in SORN A0190-45, Military Police Reporting Program Records (MRRP), that fall within 5 U.S.C. 552a(j)(2) are exempt from the requirement in 5 U.S.C. 552a (e)(3) to provide a PAS.

2-4. Administration of expelled or barred persons file

a. When action is completed by an installation commander to bar an individual from the installation under 18 USC 1382, the installation PM or DES will be provided with—

(1) A copy of the letter or order barring the individual.

- (2) Reasons for the bar.
- (3) Effective date of the bar and period covered.

b. The installation PM or DES will maintain a list of barred or expelled persons. When the bar or expulsion action is predicated on information contained in MP investigative records, the bar or expulsion document will reference the appropriate MP record or the LER. When an LER results in the issuance of a bar letter, the installation PM or DES will forward a copy of the bar letter to Director, USACRC to be filed with the original LER. The record of the bar will also be entered into COPS, in the Vehicle Registration System (VRS) module, under “Barrings.”

2-5. Police intelligence and criminal information

a. The purpose of gathering police intelligence is to identify individuals, or groups of individuals, in an effort to anticipate, prevent, or monitor possible criminal activity. Police intelligence aids criminal investigators in developing and investigating criminal cases. The AR 195-2 designates USACIDC as having the primary responsibility to operate a criminal intelligence program. Criminal intelligence will be reported through the DA Form 190-45-SG, also known as ALERTS, and other criminal intelligence products. The crimes listed in paragraphs (1) through (9) below, as well as the reportable incidents, behavioral threat indicators, and other matters of counterintelligence interest specified by AR 381-12, will be reported to the nearest Army Counter Intelligence (CI) office—

- (1) Sedition.
- (2) Aiding the enemy by providing intelligence to the enemy.
- (3) Spying.
- (4) Espionage.
- (5) Subversion.
- (6) Treason.
- (7) International terrorist activities or material support to terrorism (MST).
- (8) Unreported contacts with foreigners involved in intelligence activities.
- (9) Unauthorized or intentional disclosure of classified information.

b. Information on persons and organizations not affiliated with DOD will not normally be acquired, reported, processed, or stored. Situations justifying acquisition of this information include, but are not limited to—

- (1) Theft, destruction, or sabotage of weapons, ammunition, equipment facilities, or records belonging to DOD units or installations.
- (2) Protection of Army installations and activities from potential threat.
- (3) Information received from the FBI, State, local, or international LE agencies that directly pertain to the law enforcement mission and activity of the installation PM or DES office; the ACOM, ASCC, or DRU PMO or DES; or that has a clearly identifiable military purpose and connection. A determination that specific information will not be collected, retained, or disseminated by intelligence activities does not indicate that the information is automatically eligible for collection, retention, or dissemination under the provisions of this regulation. The above policies are not intended—and will not be used—to circumvent any Federal law that restricts gathering, retaining, or dissemination of information on private individuals or organizations.

c. Retention and disposition of information on non-DOD affiliated individuals and organizations are subject to the provisions of AR 380-13 and AR 25-400-2.

d. If a written extract from local police intelligence files is provided to an authorized investigative agency, the following will be included on the transmittal documents: “THIS DOCUMENT IS PROVIDED FOR INFORMATION AND USE. COPIES OF THIS DOCUMENT, ENCLOSURES THERETO, AND INFORMATION THEREFROM, WILL NOT BE FURTHER RELEASED WITHOUT THE PRIOR APPROVAL OF THE INSTALLATION PROVOST MARSHAL/DIRECTORATE OF EMERGENCY SERVICES.”

e. Local police intelligence files will be exempt from certain disclosure requirements by AR 25-55 and 5 USC 552 (The Freedom of Information Act), commonly known as the FOIA.

2-6. Name checks

a. Information contained in MP records will be released under the provisions of AR 340-21 to authorized personnel for valid background check purposes. Examples include child care and youth program providers, sexual assault response coordinators, unit victim advocates, access control, unique or special duty assignments, security clearance procedures, and for suitability and credentialing purposes. Any information released must be restricted to that necessary and relevant to the requester’s official purpose. The installation PMs and DESs will establish written procedures to ensure that release is accomplished in accordance with AR 340-21.

b. Checks will be accomplished by a review of DA Form 190-45-SG, also known as ALERTS. Information will be disseminated according to chapter 3 of this regulation.

c. In response to a request for local files or name checks, installation PMs and DESs will release only founded offenses with status of the disposition and what action was taken, to include if no action taken. Offenses determined to

be unfounded will not be released. These limitations do not apply to requests submitted by LE agencies for LE purposes or to CI investigative agencies for counterintelligence purposes.

d. DA Form 190–45–SG is a database called ALERTS, which contains all LERs filed worldwide. Authorized users of DA Form 190–45–SG can conduct name checks for criminal justice purposes. To conduct a name check, users must have the SSN, foreign national number, or the first and last name of the individual. If a search is done by name only, DA Form 190–45–SG, also known as ALERTS, will return a list of all matches to the data entered. Select the appropriate name from the list.

e. A successful query of DA Form 190–45–SG, also known as ALERTS, would return the following information—

- (1) The LER number.
- (2) Report date.
- (3) The SSN.
- (4) Last name.
- (5) First name.
- (6) Whether the individual has a protected identity.
- (7) A link to view the LER, DA Form 4833, and DA Form 3946 (Military Police Traffic Accident Report).
- (8) Whether the individual is a subject, victim, or a person related to the report disposition.

f. Name checks will include the criteria established in DA Form 190–45–SG, also known as ALERTS, and the USACRC. All of the policies and procedures for such checks will conform to the provisions of this regulation. Any exceptions to this policy must be coordinated with HQDA, PMG before any name checks are conducted. The following are examples of appropriate uses of the name check feature of DA Form 190–45–SG, also known as ALERTS:

- (1) Individuals named as the subjects of SIRs.
- (2) Individuals named as subjects of investigations who must be reported to the USACRC.
- (3) Employment as child care or youth program providers.
- (4) Local checks of DA Form 190–45–SG, also known as ALERTS, as part of placing an individual’s information there.
- (5) Name checks for individuals employed in law enforcement positions.

g. The installation PM or DES will ensure that an audit trail is established and maintained for all information released from MP records.

h. Procedures for the conduct of name checks with the USACRC are addressed in AR 195–2. The following information is required for USACRC name checks (when only the name is available, USACRC should be contacted telephonically for assistance)—

- (1) Full name, date of birth, SSN, and former Service number of the individual concerned.
- (2) The specific statute, directive, or regulation on which the request is based, when requested for other than criminal investigative purposes.

i. Third party checks (first party asks second party to obtain information from third party on behalf of first party) will not be conducted.

2–7. Registration of sex offenders on Army installations (inside and outside the continental United States)

a. Garrison commanders will ensure that all sex offenders (in accordance with para *b*, below) that reside or are employed on an Army installation, register with the installation PM or DES. This includes Servicemembers, civilian employees, accompanying dependent Family members, and contractors, subject to the incorporation of the sex offender registration requirement into the contract.

b. A sex offender is defined as—

(1) Any person, including but not limited to a Service member, Service member’s Family member, civilian employee, civilian employee’s family member, or contractor, who either is registered or required to register as a sex offender by any law, regulation or policy of the United States, the Department of Defense, the Army, a State, the District of Columbia, the Commonwealth of Puerto Rico, Guam, America Samoa, The Northern Mariana Islands, the U.S. Virgin Islands, or a Federally recognized Indian tribe. This definition is not limited to persons convicted for felony sex offenses but includes all persons who are registered or required to register as a sex offender regardless of the classification of their offenses, including felonies, misdemeanors, and offenses not classified as a felony or misdemeanor.

(2) The persons who are sex offenders as defined in paragraph *b*(1) include those convicted by a foreign government of an offense equivalent or closely analogous to a covered offense under the Uniform Code of Military Justice as provided in AR 27–10. See 42 USC 16911(5)(B) and U.S. Department of Justice, Office of the Attorney General, The National Guidelines for Sex Offender Registration and Notification, Final Guidelines, 73 FR 38030, 38050–1 (July 2, 2008) for guidelines and standards. Contact the servicing Office of the Staff Judge Advocate for assistance in interpreting or applying this provision.

c. Sex offenders, as defined in subparagraph *b*, must register with the installation PMO or DES within 3 working

days of first arriving on an installation. Sex offenders must provide the installation PMO or DES with evidence of the qualifying conviction. The PMO or DES will enter the registering sex offender's conviction information on a raw data file (RDF) as an information entry into DA Form 190-45-SG, also known as ALERTS, with the State the sex offender was convicted, date of conviction, and results of conviction, to include length of time required to register and any specific court ordered restrictions. Registration with the PMO or DES does not relieve sex offenders from their legal obligation to comply with applicable State and local government registration requirements for the state in which they reside, work, or attend school. (See AR 190-47 and AR 27-10.) Registration with the State is also required under 42 USC 16901 et seq. (The Sex Offender Registration and Notification Act), and implemented by AR 27-10 and DODI 1325.07. In addition, upon assignment, reassignment, or change of address, sex offenders will inform the installation PM or DES within three working days. Failure to comply with registration requirements is punishable under Federal or State law and/or under the UCMJ. "State" in this paragraph includes any jurisdiction listed in paragraph *b* of this section in which a sex offender is required to register.

d. Installation PMOs and DESs will—

(1) Maintain and update a monthly roster of current sex offenders' names and provide it to the Sexual Assault Review Board; the ACOM, ASCC and DRU PMs and DESs; and the garrison commander.

(2) Notify gaining PMs or DESs when a Soldier who is a sex offender out-processes the installation PMO or DES, and provide a copy of the DD Form 2791 (Notice of Release/Acknowledgement of Convicted Sex Offender Registration Requirements), if applicable, and RDF to the gaining installation PM or DES, ensuring compliance with applicable privacy and information handling policies.

e. DOD civilians, contractors, and Family members that fail to register at the installation PMO or DES are subject to a range of administrative sanctions, including but not limited to, a complete or limited bar to the installation and removal from military housing.

f. Installation PMs and DESs must be familiar with applicable State registration requirements for sex offenders. Installation PMs and DESs will coordinate with the local SJA and local LE agencies to identify and register those sex offenders required to register on the installation.

(1) Installation PMs or DESs will complete the following procedures for Soldier sex offender registration—

(a) Obtain a completed DD Form 2791 from trial counsel when a Soldier is convicted at a special or general courts martial of a qualifying offense but the sentence does not include any term of confinement. The installation PM or DES will ensure that a copy of the DD Form 2791 is filed with the USACRC, along with any report of investigation related to the qualifying conviction.

(b) Provide all military sex offenders with the "State registration" document(s), available through State and local LE agencies for use in registration. Direct the Soldiers to the local or State law enforcement agency, which will register them based on their physical residence address and subsequently notify the installation to which they are assigned. Installation PMs and DESs in the United States will provide written notice of the conviction or transfer to the offender's gaining unit commander, the State's chief LE officer, the chief LE officer of the local jurisdiction in which the accused will reside, the State or local agency responsible for the receipt or maintenance of a sex offender registration where the person will reside, and upon request, governmental officials of foreign countries. Installation PM and DES notifications to State and local officials are described in DODI 1325.07.

(c) Complete an RDF as an information entry into DA Form 190-45-SG, also known as ALERTS, using the "9Q" offense code.

(d) Complete the "Subject" section on the RDF, to identify the sex offender. Ensure the sex offender produces either evidence of their qualifying conviction or their sex offender registration paperwork in order to complete the "Narrative" with the state where the sex offender was convicted, date of conviction, and results of conviction, to include length of time required to register and any specific court ordered restrictions.

(e) Provide written notice to State and local LE agencies of the arrival of an offender to their local area.

(2) Installation PMs and DESs will complete the following procedures for all other sex offenders required to register on the installation—

(a) Complete an RDF as an information entry into DA Form 190-45-SG, also known as ALERTS, using the "9Q" offense code.

(b) Complete the "Subject" section on the RDF to identify the sex offender. Ensure the sex offender produces either evidence of the qualifying conviction or the sex offender registration paperwork in order to complete the "Narrative" with the state in which the sex offender was convicted, date of conviction, and results of conviction, to include length of time required to register and any specific court ordered restrictions.

2-8. Collection of deoxyribonucleic acid

a. Army LE personnel will collect deoxyribonucleic acid (DNA) pursuant to DODI 5505.14. Per this regulation, a sample of an individual's DNA is to allow for positive identification and to provide or generate evidence to solve crimes through database searches of potentially matching samples. DNA samples will not be collected from juveniles.

b. Army LE investigators (MPs, CID agents, MP investigators, and DA civilian police detectives) must consult their

servicing staff judge advocate to determine whether they are within the geographic jurisdiction of a Federal District Court that has held the collection of DNA, under 42 USC 14135a(a)(1)(a), to be unconstitutional.

c. Installation PMs and DESs will request and fund the DNA database collection kits from USACIL.

d. Once DNA samples are taken, installation PMs and DESs must ensure DNA samples are expeditiously forwarded to USACIL.

e. Army LE personnel will forward DNA samples taken from Soldiers to USACIL if one of the following circumstances exists—

(1) An Army LE investigator obtains a probable cause opine/concurrence from JAG concluding that there is probable cause that a subject being fingerprinted committed an offense identified in table 4-1, below. LE personnel will take DNA from all drug offenders, except those who are arrested or detained for the offenses of simple possession and personal use (UCMJ, Art. 112a). However, LE personnel will take DNA from these excluded offenders when charges are preferred for or the subjects are convicted at special or general court-martial of simple possession or use.

(2) The investigator may collect DNA samples prior to consulting a judge advocate but will not forward the samples to USACIL until probable cause is determined based on judge advocate consultation.

(3) When court-martial charges are preferred, in accordance with Rule for Court-Martial 307, and if any LE personnel have not previously obtained and submitted a DNA sample.

(4) When a Soldier is ordered into pre-trial confinement by a competent military authority after a commander completes the 72-hour memorandum required by Rule for Courts-Martial 305(h)(2)(c), and if LE has not previously obtained and submitted a DNA sample.

(5) When a Soldier is confined to a military correctional facility or temporarily housed in civilian facilities, as a result of a general or special court-martial conviction, and if LE have not previously obtained and submitted a DNA sample.

f. Army LE personnel will obtain a DNA sample from a civilian in their control at the point it is determined there is probable cause to believe the detained person violated a Federal statute equivalent to the offenses identified in table 4-1, except for the listed violations that are exclusively military offenses. For the purposes of this regulation, DNA shall be taken from all civilian drug offenders, except those who are arrested or detained for the offenses of simple possession and personal use. When Army LE personnel make a probable cause determination concerning a civilian not in their control, Army LE personnel are not required to collect DNA samples. Likewise, Army LE personnel are not required to obtain DNA samples when another LE agency has, or will, obtain the DNA.

g. Army LE personnel will use the USACIL DNA database collection kit, which includes a DNA sample card and the USACIL DNA database collection eform, to collect DNA samples in accordance with this regulation. Army LE personnel will document, in the appropriate case file, when civilian LE agencies handle any aspect of the DNA processing and whether the civilian LE agency forwarded the DNA sample to the FBI laboratory.

(1) Army LE personnel will complete the DNA database collection kit training program prior to using the kit. The training presentation CD is included in the kit. It is also available on the USACIL portal at <https://usacil.forscom.army.mil/codis/default.aspx>.

(2) Army LE personnel will ensure The Privacy Act Statement and Notice of the General Rights for Requesting Expungement (both are included in the USACIL kit) are provided to subjects when DNA samples are collected.

(3) The kit includes a pink DNA sample card and data card. Army LE personnel will write the SSN or any available means of identification (license number; resident number) of the individual whose DNA is being taken on both the back of the DNA sample card and data card. The LER will be entered on the data card.

h. Expungement procedures include the following—

(1) Soldiers may request, in writing, that their DNA records be expunged if their DNA sample was taken but they are not convicted of any offense by general or special courts-martial (including action generally inconsistent with such conviction, such as administration of nonjudicial punishment, administrative separation, or referral to a summary court).

(a) Soldiers must forward requests for expungement through the first commanding officer in the grade of major, or higher, in the Soldier's chain of command. Requests must include proof that charges were dismissed, withdrawn, disposed of in a manner not resulting in preferral of charges pursuant to RCM 307, or otherwise did not or will not result in a conviction of any offense (including proof of action by a general or special court-martial convening authority resulting in full acquittal).

(b) The first commanding officer in the grade of major or higher then reviews, confirms the information, and submits the request through the installation PM or DES.

(c) Installation PMs and DESs then receive the expungement requests and must ensure Soldiers have no convictions prohibiting the expungement. Installation PMs and DESs must provide a memorandum to USACIL stating that the individual is entitled to expungement. Requests must be on letterhead and bear the title, signature, and telephone number of the Army LE personnel submitting the request, as well as the Soldier's full name, SSN, and mailing address. Requests must include all documents submitted by the member, along with additional relevant documents in the possession of the commander or official receiving the request. Installation PMs and DESs will forward the memorandum to the attention of the Combined DNA Index System Branch chief at USACIL for action. The Army LE

organization will maintain a copy of requests for expungement in the case file. This includes those requests not forwarded to USACIL because expungement was not appropriate.

(d) Installation PMs and DESs will forward to USACRC the expungement request memoranda and associated documentation to be included in the case file.

(e) If the commanding officer, after consulting with a judge advocate, determines that expungement is not authorized, the commander notifies the requestor in writing with a copy furnished to the Army LE organization.

(2) The DODI 5505.14 details the procedures former Soldiers and civilians must follow to request expungement of their DNA records. Former Soldiers and civilians from whom DNA samples have been taken, but were not convicted, do not submit requests to have their DNA record expunged through installation PMO or DES channels. To request expungement of DNA records for civilians pursuant to Sections 14132 of Title 42, United States Code, the requestor or legal representative must submit a written request to: FBI Laboratory Division, 2501 Investigation Parkway, Quantico, VA 22135, Attention: Federal Convicted Offender Program Manager.

i. This policy does not eliminate other legal or policy requirements to provide DNA, fingerprints, or criminal history data, including submissions to the Defense Incident-Based Reporting System (DIBRS). DNA expungement allowed by this policy does not also allow the expungement of DNA gathered under any other legal, policy, or administrative requirements.

j. This policy does not affect OPMG policies and procedures for the identification, collection, and retention of biological and other physical evidence during the course of an investigation.

2–9. Armed escorts and unique Federal agency number documentation

In compliance with AR 190–30 and AR 25–400–2, the installation PMO or DES will ensure the completion and submission of LER and supporting documentation in DA Form 190–45–SG, also known as ALERTS, and to USACRC for all armed escorts of Soldiers who are absent without leave (AWOL), deserters, and military prisoners. The installation PMO or DES will add an information entry into the blotter records of AWOL and prisoner escorts by law enforcement. Supporting documents must include—

a. Colonel-level commander's armed escort approval and a unique Federal agency number request memorandum (if using commercial air).

b. The DD Form 2977 (Deliberate Risk Assessment Worksheet). For use of the form, see ATP 5–19.

c. The DA Form 7630 (Department of the Army Law Enforcement Escort Credential). For use of the form, see AR 190–9.

d. A completed DA Form 4833.

e. Absentee and deserter documents as applicable—

(1) The DD Form 553 (Deserter/Absentee Wanted by the Armed Forces).

(2) The DD Form 616 (Report of Return of Absentee).

(3) The LER.

f. Prisoner documents as applicable—

(1) The DD Form 2707 (Confinement Order). For use of the form, see AR 190–47.

(2) Assignment orders (identification of confinement or correctional facility).

(3) Result of Trial.

Chapter 3 Release of Information

3–1. General

a. The policy of HQDA is to conduct activities in an open manner and provide the public accurate and timely information. Accordingly, LE information will be released to the degree permitted by law and Army regulations. The public affairs officer (PAO) must be informed of information released outside the local jurisdiction, and the PAO must be included as a trusted agent on communications between the installation PM, or DES, and the commander (see AR 360–1).

b. Any release of MP records or information compiled for LE purposes, whether to persons within or outside the Army, must be in accordance with the FOIA and The Privacy Act.

c. Requests by individuals for access to MP records about themselves will be processed in compliance with AR 25–55 and AR 340–21.

d. The MP records in the temporary possession of another organization remain the property of the originating LE agency. The following procedures apply to any organization authorized temporary use of MP records—

(1) Any request from an individual seeking access to MP records must be immediately referred to the originating LE agency for processing. The temporary custodian of MP records does not have the authority to release those records.

(2) When the temporary purpose of the using organization has been satisfied, the MP records will be returned to the originating law enforcement agency or the copies will be destroyed.

(3) A using organization will maintain information from MP records in their system of records, if approval is obtained from the originating LE agency. This information will include reference to an MP record (for example, LER number or date of offense), a summary of information contained in the record, or the entire MP record. When a user includes an MP record in its system of records, the originating LE agency must delete portions from that record to protect special investigative techniques, maintain confidentiality, preclude compromise of an investigation, and protect other LE interests.

3-2. Guidelines for disclosure within the Department of Defense

a. Criminal record information contained in MP documents will not be disseminated unless there is a clearly demonstrated, official, need to know. A demonstrated, official, need to know exists when the record is necessary to accomplish a function that is within the responsibility of the requesting activity or individual, is prescribed by statute, DOD directive, regulation, or instruction, or by Army regulation.

(1) Criminal record information will be disclosed to commanders or staff agencies to assist in executing criminal justice functions. Only that information reasonably required will be released. Such disclosure must clearly relate to a LE function.

(2) Criminal record information related to subjects of criminal justice disposition will be released when required for security clearance procedures.

(3) Criminal record information will be released to an activity when matters of national security are involved.

(4) When an individual informs an activity of criminal record information pertaining to him or her, the receiving activity will seek verification of this information through the responsible LE agency or will forward the request to that organization. The individual must be advised by the receiving agency of the action being pursued. Law enforcement agencies will respond to such requests in the same manner as with requests under FOIA and The Privacy Act.

(5) Army Directive 2013-06, dated 14 February 2013, authorizes brigade-level or higher commanders (0-6 or above) to receive criminal history reports, stored in Army law enforcement systems, on newly assigned Soldiers. The criminal history checks involve Soldiers in a permanent change of station, intra-installation or intra-theater reassignment. The criminal history checks will identify all founded offenses, to include any known adjudication, over the last 5 years of the Soldiers' time in service.

b. Nothing in this regulation will be construed to limit the dissemination of information between military police, the USACIDC, and other LE agencies within the Army and DOD.

c. Information released within the DOD must be structured to support DOD guidance on net-centric data sharing implementation, under DOD 8320.02-G, and must conform to the standards, principles, and business rules in the common operating environment.

3-3. Release of information

a. Release of information from Army records to agencies outside DOD will be governed by AR 25-55, AR 340-21, AR 600-37, and this regulation. Procedures for release of certain other records and information is contained in AR 20-1, AR 27-20, AR 27-40, AR 40-66, AR 195-2, AR 360-1, and AR 600-85. Installation drug and alcohol offices will be provided an extract of the RDF for offenses involving the use of alcohol or drugs (for example, drunk driving, drunk and disorderly conduct, or a positive urinalysis).

b. Installation PMs and DESs are the release authorities for MP records under their control. They release criminal record information to other activities as prescribed in AR 25-55, AR 340-21, and this regulation.

c. Authority to deny access to criminal records information rests with the initial denial authority for the FOIA and the denial authority for Privacy Act cases, as addressed in AR 25-55 and AR 340-21.

3-4. Release of information under the Freedom of Information Act

a. The release and denial authorities for all FOIA requests concerning MP records include installation PMs, DESs, and the Commander, USACIDC. Authority to act on behalf of the Commander, USACIDC is delegated to the Director, USACRC.

b. FOIA requests from members of the press will be coordinated with the installation PAO prior to release of records under the control of the installation PM or DES. When the record is on file at the USACRC, the request must be forwarded to the Director, USACRC.

c. Requests will be processed as prescribed in AR 25-55 and as follows—

(1) The installation FOIA Office reviews requested reports to determine if any portion is exempt from release.

(2) Statutory and policy questions will be coordinated with the local SJA.

(3) Coordination will be completed with the local USACIDC activity to ensure that the release will not interfere with a criminal investigation in progress or affect final disposition of an investigation.

(4) If it is determined that a portion of the report or the report in its entirety will not be released, the request to include a copy of the LER or other MP records will be forwarded to the Director, USACRC (CICR-FP), 27130

Telegraph Road, Quantico, VA 22134. The requestor will be informed that the request has been sent to the Director, USACRC, and provided the mailing address for the USACRC. When forwarding FOIA requests, the outside of the envelope must be clearly marked "FOIA REQUEST."

(5) A partial release of information by an installation FOIA Office is permissible when it is acceptable to the requester. (An example would be the redaction of a third party's SSN, home address, and telephone number, as permitted by law.) If the requester agrees to the redaction of exempt information, such cases do not constitute a denial. If the requester insists on obtaining the entire report, then a copy of the report and the request for release will be forwarded to the Director, USACRC. There is no requirement to coordinate such referrals at the installation level. The request is simply forwarded to the Director, USACRC for action.

(6) Requests for MP records that have been forwarded to USACRC and are no longer on file at the installation PMO or DES must be forwarded to the Director, USACRC for processing.

(7) Requests concerning USACIDC reports of investigation or USACIDC files will be referred to the Director, USACRC. In each instance, the requestor will be informed of the referral and provided the address for the Director, USACRC.

(8) Requests concerning records that are under the supervision of an Army activity, or other DOD agency, will be referred to the appropriate agency for response.

3-5. Release of information under The Privacy Act of 1974

a. The MP records will be released according to provisions of The Privacy Act of 1974, as implemented by AR 340-21 and this regulation.

b. The release and denial authorities for all Privacy Act cases concerning MP records are provided in paragraph 3-3, of this regulation.

c. Privacy Act requests for access to a record, when the requester is the subject of that record, will be processed as prescribed in AR 340-21.

3-6. Amendment of records

a. *Policy.* An amendment of records is appropriate when such records are established as being inaccurate, irrelevant, untimely, or incomplete. Amendment procedures are not intended to permit challenging an event that actually occurred. Requests to amend reports will be granted only if the individual submits new, relevant and material facts that are determined to warrant their inclusion in or revision of the police report. The burden of proof is on the individual to substantiate the request. Requests to delete a person's name from the title block will be granted only if it is determined that there is not probable cause to believe that the individual committed the offense for which he or she is listed as a subject. It is emphasized that the decision to list a person's name in the title block of a police report is an investigative determination that is independent of whether or not subsequent judicial, nonjudicial or administrative action is taken against the individual. In compliance with DOD policy, an individual will still remain entered in the Defense Clearance Investigations Index (DCII) to track all reports of investigation.

b. *Procedures.*

(1) Installation PMs or DESs will review amendment requests. Upon receipt of a request for an amendment of a MP record that is 5 or fewer years old, the installation PM or DES will gather all relevant available records at the installation. The installation PM or DES then reviews the request and either approves it or forwards it to the Director, USACRC with a recommendation and rationale for denial. In accordance with AR 340-21, the Commanding General, USACIDC is the sole access and amendment authority (AARA) for criminal investigation reports and LERs. Access and amendment refusal authority is delegable, in writing, pursuant to 32 CFR 505.5(i)(2)(i), to a division chief in the grade of GS-14/O5 or higher, under the supervision of the AARA. If the decision is made to amend an LER, a supplemental LER is prepared. The supplemental LER will change information on the original LER and must be mailed to the Director, USACRC with the amendment request from the requestor as an enclosure. The Director, USACRC then files the supplemental LER with the original LER and notifies the requestor of the amendment of the LER.

(2) Requests to amend MP documents that are older than 5 years will be coordinated through the Director, USACRC. The installation PM or DES will provide the Director, USACRC a copy of an individual's request to amend a MP record on file at the USACRC. If the Director, USACRC receives an amendment request, the correspondence with any documentation on file at the USACRC will be sent to the originating installation PMO or DES. The installation PM or DES will review the request and either approve the request or forward it to the Director, USACRC for denial. A copy of the installation PM or DES's decision must be sent to the Director, USACRC to be filed in the USACRC record. If an amendment request is granted, copies of the supplemental LER must be provided to each organization, activity, or individual who received a copy of the original LER.

(3) If the installation PMO or DES no longer exists, the request will be staffed with the IMCOM region, ACOM, ASSC, or DRU PMO or DES that had oversight responsibility for the installation PMO or DES at the time the LER was originated.

3-7. Accounting for military police record disclosure

- a. The AR 340-21 prescribes accounting policies and procedures concerning the disclosure of MP records.
- b. The installation PMs and DESs will develop local procedures to ensure that disclosure of MP records as described in AR 340-21 are available on request.
- c. In every instance where records are disclosed, the individuals, agencies, or components are reminded that use or further disclosure of any MP reports, military police investigator's reports, or other information received must be in compliance with DODI 5505.7, paragraph 6.5.2., which states that "judicial or adverse administrative actions shall not be taken against individuals or entities based solely on the fact that they have been titled or indexed due to a criminal investigation."

3-8. Release of law enforcement information furnished by foreign governments or international organizations

- a. Information furnished by foreign governments or international organizations is subject to disclosure, unless exempted by AR 25-55, AR 340-21, Federal statutes, or executive orders.
- b. Release of U.S. information (classified military information or controlled unclassified information) to foreign governments is accomplished in accordance with AR 380-10.

3-9. Release of domestic incidents reports to the Army Family Advocacy Program

- a. Installation PMO or DES will comply with the reporting requirements in accordance with AR 608-18.
- b. In addition to substantiated incidents of domestic violence, the installation PM or DES will notify the family advocacy program manager and social work services of all incidents in which a preponderance of indicators reveal a potential risk of reoccurrence and increasing severity of maltreatment, which could lead to domestic violence or child abuse. Installation PMs and DESs will ensure these notifications are recorded in the official MP journal in DA Form 190-45-SG, also known as ALERTS. This is done to—
 - (1) Establish a history of incidents that indicate an emerging pattern of risk of maltreatment or victimization to Soldiers and/or Family members. See AR 608-18 for incidents that indicate maltreatment.
 - (2) Develop a trend history of unsubstantiated or unresolved incidents, in order to prevent possible violence or maltreatment from occurring.

Chapter 4 Offense Reporting

4-1. General

- a. This chapter establishes policy for reporting founded criminal offenses investigated by Army installation offices; any ACOM, ASCC, or DRU's PM or DES offices; and the IMCOM.
- b. This chapter prescribes reporting procedures, which require the use of DA Form 190-45-SG and a systems administrator to ensure that the system is properly functioning. Reporting requirements include—
 - (1) Reporting individual offenders to the USACRC, NCIC, CJIS, and the DOD.
 - (2) Sending crime reports to the DOD. The DOD collects data from all the Services using the DIBRS. The Army inputs its data into DIBRS, using DA Form 190-45-SG, also known as ALERTS. Any data reported to DIBRS is only as good as the data reported in DA Form 190-45-SG, also known as ALERTS, so the need for accuracy in reporting incidents and using proper offense codes is critical. The DIBRS data from DOD is eventually sent to the DOJ's National Incident-Based Reporting System (NIBRS). The data is eventually incorporated within the uniform crime report (UCR).
- c. An installation PMO or DES initiating an LER or other Army LE investigation has reporting responsibility explained throughout this regulation and will refer to AR 195-2 for a list of offense investigative responsibilities.
- d. In the event the installation PMO or DES determines that his or her office does not have investigative responsibility or authority, the LER will be terminated and the case cleared by exceptional clearance. A case cleared by exceptional clearance is closed by the installation PMO or DES when no additional investigative activity will be performed, or when the case is referred to another agency. If a case is transferred to the installation PMO or DES, from another LE investigation agency, the gaining installation PMO or DES will have all reporting responsibility using the DA Form 190-45-SG, also known as ALERTS.

4-2. Law Enforcement Report

- a. *General use.* The LER is used to—
 - (1) Record all information or complaints received or observed by the installation PMO or DES.
 - (2) Serve as a record of all installation PMO or DES activities.
 - (3) Document entries made into DA Form 190-45-SG, also known as ALERTS, and other automated systems.

(4) Report information concerning investigations conducted by civilian LE agencies related to matters of concern to the Army.

(5) Advise commanders and supervisors of offenses and incidents involving personnel or property associated with their command or functional responsibility.

(6) Report information developed by commanders investigating incidents or conducting inspections that result in the disclosure of evidence that a criminal offense has been committed.

b. Special use. The LER will be used to—

(1) Transmit a completed DA Form 3946 (Military Police Traffic Accident Report). This will include statements, sketches, or photographs that are sent to a commander or other authorized official.

(2) Transmit the Central Violations Bureau (CVB) Form when required by local installation or U.S. Magistrate Court policy. The LER is used to advise commanders or supervisors that military, civilian, or contract personnel have been cited on a Central Violations Bureau Form.

(3) Match individual subjects with individual victims or witnesses and founded criminal offenses. This is a Federal statutory requirement. This is done using the “relationships” tab within DA Form 190–45–SG, also known as ALERTS.

(4) Document victim or witness liaison activity.

(5) Indicate confirmation of command notification, and medical and nonmedical notification, as applicable (such as a physician, ASAP, (AFAP) (social services), a chaplain, local prosecutors, or LE), prior to release of subjects.

c. Distribution. The LER will be prepared in three copies, signed by the installation PMO, DES, or a designated representative, and distributed as follows—

(1) Send the original to USACRC. Further information, arising or developed at a later time, will be forwarded to USACRC using a supplemental LER. Reports submitted to USACRC will include a good, legible copy of all statements, photographs, sketches, laboratory reports, and other information that substantiates the offense or improves understanding of the report. The USACRC control number must be recorded on every LER sent to the USACRC. A report will not be delayed for adjudication or commander’s action beyond 60 days.

(2) One copy is retained in the installation PMO or DES files.

(3) One copy is forwarded through the field grade commander to the immediate commander or supervisor of each subject or organization involved in an offense.

d. Changing reports for unfounded offenses. If an offense is determined to be unfounded, after the case has been forwarded to USACRC, the following actions will be completed—

(1) A supplemental LER, using the same LER number and USACRC control number, will be submitted stating the facts of the subsequent investigation and that the case is unfounded.

(2) A copy of the supplemental LER will be provided to those agencies or activities that received a copy of the completed LER at the time of submission to USACRC and to the commander for action.

e. “Redacted” copy. When sending the LER to outside agencies, generate or print a “redacted” LER from the automated DA Form 190–45–SG, also known as ALERTS.

4–3. Identifying criminal incidents and subjects of investigation

a. An incident will not be reported as a founded offense unless adequately substantiated by police investigation. A person or entity will be reported as the subject of an offense on the LER when credible information exists that the person or entity has committed a criminal offense. The decision to title a person is an operational, rather than a legal, determination. The act of titling and indexing does not, in and of itself, connote any degree of guilt or innocence; rather, it ensures that information in a report of investigation can be retrieved at some future time for LE and security purposes. Judicial or adverse administrative actions will not be based solely on the listing of an individual or legal entity as a subject on the LER.

b. The PMO, DES, and USACIDC offices must remind commanders that, in accordance with AR 600–8–2, suspending favorable personnel actions is mandatory when an investigation (formal or informal) is initiated on a Soldier by military or civilian authorities. In addition, commanders will report investigations to their security manager to ensure reporting of derogatory incidents are sent to the DOD Consolidated Adjudication Facility via the Joint Personnel Adjudication System, as outlined in AR 380–67.

c. An MP LER is reportable to the USACRC when a subject of an included offense is identified, the offense is founded, and the offense is punishable by confinement of 6 months or more. Not all suspects for a particular offense need be identified for that offense to be categorized as a founded offense. A subject can be a person, corporation, or other legal entity about which credible information exists that would cause a trained investigator to presume that the person, corporation, or other legal entity committed a criminal offense.

d. When investigative activity identifies a subject, all facts of the case must be considered. When a person, corporation, or other legal entity is entered in the “subject” block of the LER, their identity is recorded in DA automated systems and the DCII. Once entered into the DCII, the record can only be removed in cases of mistaken identity or if an error was made in applying the credible information standard at the time of listing the entity as a subject of the report. It is emphasized that the credible information error must occur at the time of listing the entity as

the subject of the LER rather than subsequent investigation determining that the LER is unfounded. This policy is consistent with DOD reporting requirements. The Director, USACRC enters individuals from the LER into the DCII.

e. The USACRC control numbers are automatically assigned within the DA Form 190–45–SG, also known as ALERTS. Once assigned, a USACRC number can only be deleted by the Crime Records Center. For MP units in immature theaters (such as contingency operations, deployed environments, and so forth), the USACRC control numbers will be manually assigned and made available by the USACRC until the DA Form 190–45–SG, also known as ALERTS, becomes operational or USACRC control numbers are no longer required.

4–4. Offense codes

Each offense code describes, as nearly as possible, the complaint or offense by using an alphanumeric code. A chart listing the offense codes that are authorized for use within the Army is available at appendix C. This list will be amended from time to time, based on new reporting requirements mandated by legislation or administrative procedures. The IMCOM, ACOM, ASCC, and DRU commanders, and the installation PMOs and DESs, will be notified by special letters of instruction issued in numerical order from the OPMG when additions or deletions are made to the list. The DA Form 190–45–SG, also known as ALERTS, will be used for all reporting requirements.

4–5. Military police codes

a. Military police codes (MPCs) identify individual PMOs and DESs. The Director, USACRC will assign MPCs to PMOs and DESs.

b. Requests for assignment of a MPC will be included in the planning phase of military operations, exercises, or missions when LE operations are anticipated. The request for a MPC will be submitted as soon as circumstances permit, without jeopardizing the military operation to HQDA, OPMG. Consistent with security precautions, the IMCOM, ACOM, ASCC, and DRU immediately informs HQDA, OPMG when assigned or attached MP units are notified for deployment, mobilization, relocation, activation, or inactivation.

c. When an MP unit is alerted for deployment to a location not in an existing PMO or DES's operational area, the receiving combatant commander will request assignment of an MPC number from HQDA, OPMG providing the area of operations does not have an existing MPC number. The receiving combatant commander is further responsible for establishing an operational DA Form 190–45–SG system, also known as ALERTS, for the deployment.

4–6. Reserve component, U.S. Army Reserve, and Army National Guard personnel

a. When in a military duty status pursuant to official orders (Federal status for ARNG), Reserve and ARNG personnel will be reported as active duty. Otherwise, they will be reported as Reserve and National Guard Soldiers.

b. The LER and DA Form 4833 will be forwarded directly to Commander, USAR (ARRC–JAM), 4710 Knox Street, Building 8–1808, Fort Bragg, NC 28310–5010 for Reserve Soldiers. For ARNG Soldiers, a copy of the LER will be sent to the Director, Army National Guard, 1411 Jefferson Davis Highway, Arlington VA 22202–3231.

4–7. DA Form 4833 (Commander's Report of Disciplinary or Administrative Action)

a. Form use. The DA Form 4833 is used with the LER to—

- (1) Record actions taken against identified offenders.
- (2) Report the disposition of offenses investigated by civilian LE agencies.

b. Preparation by the installation PMO or DES office. The installation PMO or DES initiates this critical document and is responsible for its distribution and for establishing a suspense system to ensure timely response by commanders. Disposition reports are part of the reporting requirements within DA, DOD, and DOJ. The installation PM, DES, and CID offices then send the DA Form 4833 to the subject's unit commander for completion; they also copy furnish the brigade judge advocate and the subject's brigade commander.

c. Completion by the unit commander. Company, troop, and battery level commanders are responsible and accountable for completing DA Form 4833 with supporting documentation in all cases investigated by MP, civilian detectives employed by the DA, and the installation PMO or DES. The battalion commander or the first lieutenant colonel in the chain of command is responsible and accountable for completing DA Form 4833 with support documentation (copies of investigations under UCMJ, Article 15; court-martial orders; reprimands; and so on) for all USACIDC investigations. The commander completes the DA Form 4833 within 60 days of receipt and returns it to the originating office (the installation PMO, DES, or CID).

d. Appropriate blocks for completion. Commanders will complete the information in the appropriate blocks on the DA Form 4833. The appropriate blocks or blanks will be completed as indicated below—

(1) Action taken (for example, judicial, nonjudicial, or administrative). In the event the commander takes action against the Soldier for an offense other than the one listed on the LER, the revised charge or offense will be specified in the "Remarks" section of the DA Form 4833.

(2) Sentence, punishment, or administrative action imposed.

(3) Should the commander take no action, the DA Form 4833 must be annotated to reflect that fact.

e. Extenuating circumstances. If extenuating circumstances prevent the commander from completing the DA Form

4833 within 60 days of receipt, the brigade-level commander will notify the installation PMO or DES of the status and request an extension. The installation PM or DES will notify the garrison commander and the senior commander of delinquent DA Forms 4833 monthly.

(1) There is no requirement for the DA Form 4833 to be completed before the installation PMO or Directorate of Emergency Services submits the completed LER to the USACRC. The DA Form 4833 is, however, desired when submitting FBI Form FD 249 (CJIS Fingerprint Supply/Requisition Form) and/or FBI Form R-84 (Final Disposition Report), to the USACRC.

(2) A delay will have an impact on other reporting requirements (for example, submitting fingerprint cards to the FBI).

f. Procedures when subjects are reassigned. When the subject of an offense is reassigned, the installation PM or DES will forward the LER, DA Form 4833, and all pertinent attachments to the gaining installation PM or DES, who must ensure that the new commander completes the document. Copies of the documents will be made and retained by the processing PM or DES before returning the documents to the losing installation PM or DES for completion of automated entries and required reports.

g. Report on subjects assigned to other installations. When the LER involves a subject who is assigned to another installation, the initiating installation PM or DES will forward the original and two copies of DA Form 4833 to the PM or DES of the installation where the Soldier is permanently assigned.

h. Offenses not reportable to Army Crime Records Center. When the offense is not within a category reportable to USACRC, the original DA Form 4833 is retained by the installation PM or DES.

i. Civilian court proceedings. If a Soldier is tried in a civilian court, and the installation PMO or DES is notified of the charges, the installation PMO or DES will initiate an LER and forward the LER and related documents to the installation SJA court liaison to track the disposition. The installation PMO or Directorate of Emergency Services will coordinate with SJA and commanders for final disposition and report the disposition on DA Form 4833 as appropriate. The installation PMO, DES, or other designated person will sign DA Form 4833 before forwarding it to USACRC.

j. Civilian subjects titled by Army law enforcement. The PMO, DES, and USACIDC offices will complete and submit FBI Form R-84 (Final Disposition Report) to USACRC for civilian subjects, not subject to UCMJ, who are titled by Army law enforcement. The PMO or DES and USACIDC will complete the DA Form 4833 and submit the form to USACRC for these subjects. The PMO or DES and USACIDC law enforcement will not include these completed DA Forms 4833 for civilian personnel in reporting compliance statistics for commanders. This ensures records of disposition of civilian subjects titled by military LE are available in CJIS to support NCIC background checks for firearms purchases, employment, security clearances, and so on.

k. Dissemination to other agencies. A copy of the completed DA Form 4833 reflecting offender disposition will also be provided to those agencies or offices that originally received a copy of the LER when evidence is involved. The evidence custodian will also be informed of the disposition of the case.

l. Review of offender disposition by the installation Provost Marshal Office or Directorate of Emergency Services. Upon receipt of DA Form 4833 reflecting no action taken, the PM or DES will review the LER. The review will include, but is not limited to the following—

- (1) Determination of the adequacy of supporting documentation.
- (2) Contact with subject's commander to ensure all evidence presented is understood.
- (3) Whether or not coordination with the supporting SJA should have been sought prior to dispatch of the report to the commander for action.
- (4) Identification of functions that warrant additional training of MP or security personnel (for example, search and seizure, evidence handling, or rights warning).

m. Offender disposition summary reports. The installation PM or DES will provide the supported commander (normally, the general courts-martial convening authority or other person designated by proper authority) summary data of offender disposition as required or appropriate. Offender disposition summary data will reflect identified offenders on whom final disposition has been reported. This data will be provided in the format and at the frequency specified by the supported commander.

n. Reporting in the DA Form 190-45-SG (Army Law Enforcement Reporting and Tracking System (ALERTS)). An offender's disposition will be recorded in DA Form 190-45-SG, also known as ALERTS, on the DA Form 4833 that was automatically generated in DA Form 190-45-SG from the LER.

o. Administrative closures. The installation PM or DES will consult with their servicing SJA to administratively close cases older than 2 years where a commander cannot be identified. In these cases the installation PM or DES or designee will sign in block 11 and in the name portion of block 11 will annotate "reporting."

p. Commander self-initiated DA Form 4833. In accordance with DODI 7730.47 and DODM 7730.47-m, Vol.1, commanders are also responsible for completing and submitting to installation PMOs or DESs the DA Form 4833. Commanders must complete and submit DA Form 4833 for specified offenses per AR 195-2, appendix B, table B-1. Commanders must refer to Army law enforcement (Military Police Investigation or CID) every credible allegation (that is, supported by probable cause) that an assigned Soldier committed a crime that falls outside of the commander's investigative purview. If a commander initiates the DA Form 4833, the completed form will be forwarded to the

installation PMO or DES for input into DA Form 190–45–SG, also known as ALERTS. The installation PMO or DES will initiate an LER using the information on the DA Form 4833 in order to generate the DA Form 4833 in the automated DA Form 190–45–SG, also known as ALERTS.

(1) The commander will submit a self-initiated DA Form 4833 to their installation PMO/DES based on the following criteria; the commander has completed their command investigation and determined to take action against the offender. The commander will annotate the final disposition of the case on the DA Form 4833; the commander must indicate on the DA Form 4833 the type of action taken (that is, judicial punishment, nonjudicial punishment, administrative reprimand, administrative separation, counseling, and so on).

(2) Commander's self-initiated DA Form 4833 reporting process overview:

(a) If a unit commander has conducted a criminal investigation about an incident not investigated by law enforcement and meets the reporting requirements in AR 195–2, table B–1, the unit commander will access the DA Form 4833 on the Army Publishing Directorate's forms Web site and complete the relevant fields. The unit commander will email the completed and signed DA Form 4833 with the supporting documents (record of commander's inquiry, Article 15, or court-martial paperwork, and so forth) to the supporting installation PMO/DES. For commands not on an installation or commands on a Joint base, the supporting PMO/DES can be found in table 1–1 of this regulation.

(b) Installation PMO/DES will receive the DA Form 4833 from unit commanders and generate an LER from the DA Form 190–45–SG, also known as ALERTS, using the information provided in the supporting documentation. The appropriate offense code from appendix C–1 will be utilized. The first line of the narrative of the LER will state, "This is being completed and reported based on an investigation conducted by the unit commander." The PMO/DES will then copy the information provided by the commander into the DA Form 4833, generated in the automated DA Form 190–45–SG, also known as ALERTS, and close the LER.

4–8. Updating DA Form 190–45–SG (Army Law Enforcement Reporting and Tracking System (ALERTS))

The installation PMs or DESs will establish standard operating procedures to ensure that all criminal activity is reported in the electronic DA Form 190–45–SG, also known as the ALERTS database. Timely and accurate reporting is critical. If a case remains open, changes will be made as appropriate. This includes reporting additional witnesses and all aspects of the criminal report. These procedures will include but are not limited to user access, restricted or suspended access when pending an investigation, periodic name checks as deemed necessary by the installation PM or DES, training prior to be granted access and privileges into the automated DA Form 190–45–SG, proper use of the form based upon job requirements, and actions upon misuse of the form.

4–9. FBI Form R–84 and final disposition report submission requirements

In general, this paragraph implements DODI 5505.11, which prescribes procedures for Army LE to report offender criminal-history data, by submitting FBI Form FD 249 to USACRC. USACRC forwards this data to the CJIS division of the FBI, for inclusion in the Next Generation Identification Database. This paragraph does not eliminate other requirements to provide criminal-history data, including those concerning the DIBRS.

a. The installation PM or DES will submit offender criminal history data to USACRC, based on a probable cause standard determined in conjunction with the servicing SJA or legal advisor for all—

(1) Members of the military Services investigated for offenses listed in table 4–1, by any Army LE organization.

(2) Civilians investigated for offenses equivalent to those listed in table 4–1. This includes foreign nationals, persons serving with or accompanying an armed force in the field in time of declared war or contingency operations, and persons subject to Public Law 106–523 in accordance with DODI 5525.11.

(3) Military Servicemembers, their dependents, DOD employees, and contractors investigated by foreign law enforcement organizations for offenses equivalent to those listed in DODI 5505.11 and made available to any Army LE organization.

b. For purposes of this paragraph, commanders will notify their installation PMO or DES—

(1) When a military judicial proceeding is initiated or command action is taken in military nonjudicial proceedings pursuant to UCMJ, Article 15 against a military subject investigated by an Army LE organization for an offense listed in table 4–1. Offender criminal history data will not be reported in accordance with this paragraph unless the subject has been investigated by an Army LE agency for an offense listed in table 4–1. For example, if a unit investigates an alleged offense in table 4–1, and initiates a judicial and/or nonjudicial proceeding without an Army LE organization having investigated the subject, then the reporting requirements of this paragraph do not apply.

(2) When they become aware that a non-DOD and/or foreign LE organization has initiated an investigation against a Soldier, military dependent, or DOD civilian employee or contractor, for the equivalent of an offense listed in table 4–1, or punishable pursuant to the United States Code.

(3) Of the final disposition via DA Form 4833 of cases under the circumstances discussed in subparagraphs (1) and (2), above.

c. These are the fingerprint and reporting procedures—

(1) Fingerprints and all information required on FBI Form FD 249 are obtained from military subjects under

investigation by any Army LE organization for offenses listed in table 4–1. Fingerprints and additional required information pertaining to civilian subjects are obtained for offenses punishable pursuant to the United States Code, equivalent to those listed in table 4–1. Where required, a Privacy Act Statement is provided to each suspect whose personal data is collected in accordance with DOD 5400.11–R.

(2) Offender criminal history data records required in accordance with this paragraph is initiated by preparing and submitting an FBI Form FD 249 with the LER, to the Director, USACRC, CICR–CR, 27130 Telegraph Road, Quantico, VA 22134. The Director, USACRC will forward the FBI Form FD 249 to CJIS. The USACRC is used as the central repository for criminal history information in the Army. When required, Army LE organizations should submit all completed FBI Forms R–84 directly to the CJIS Division, FBI per DODI 5505.11.

(3) The originating agency identifier (ORI) identification number used on the FBI Form FD 249 will be VAUSA1400. Two FBI Forms FD 249 will be completed. One will be retained in the installation PMO or DES file. The second will be sent to the Director, USACRC, and processed with the LER. A third set of prints will also be taken on the FBI Form R–84. The FBI Form R–84 requires completion of the disposition portion and entering of the offenses on which the commander took action.

(a) For military subjects (investigated by an Army LE organization), the FBI Form FD 249 is submitted when an agent or LE official determines, following coordination with the servicing SJA or legal advisor if necessary (in no case earlier than apprehension (military), arrest (civilian), or the subject interview), that probable cause exists to believe that the person has committed an offense listed in table 4–1. If applicable, such coordination shall be documented in the investigative file.

(b) If applicable, approval of a request for discharge, retirement, or resignation in lieu of court-martial, and/or a finding of lack of mental competence to stand trial, is recorded as “final disposition” either on the FBI Form FD 249 or FBI Form R–84.

(c) Within 15 calendar days after final disposition of military judicial or nonjudicial proceedings, or the approval of a request for discharge, retirement, or resignation in lieu of court-martial, disposition information shall be reported by Army LE organizations on the FBI Form FD 249, if it has not already been reported on an FBI Form FD 249. Do not hold the FBI Form FD 249 or FBI Form R–84 pending appellate actions. Appellate action affecting the character of an initial disposition must be reported if it occurs. Dispositions that are exculpatory in nature (for example, dismissal of charges, acquittal) are also be documented on the FBI Form R–84.

(d) For civilian subjects (investigated by an Army LE organization)—

1. Submit an FBI Form FD 249 within 15 calendar days of the subject interview, arrest, indictment, or information, as applicable, for offenses punishable pursuant to the U.S. Code that are equivalent to those listed in table 4–1.

2. Submit FBI Form R–84 within 15 calendar days after sentencing.

3. In cases investigated jointly with another law enforcement organization when that organization agrees to obtain and forward fingerprints and criminal history data to the FBI, prepare a memorandum for the case file. The memorandum shall identify each subject and the law enforcement organization collecting and forwarding the data. A current memorandum of understanding at the organizational level, addressing the requirement to obtain fingerprints and associated data and to forward said information to the FBI, will suffice in lieu of case-specific memorandums. However, copies of the submitted data must be obtained for the case file.

d. Information requirements include the following—

(1) The FBI provides blank FBI Form FD 249 and/or FBI Form R–84, pre-addressed envelopes, and further guidelines for submission of criminal history data. Installation PMs and DESs are authorized to requisition the fingerprint cards by sending a request for supplies to: Federal Bureau of Investigation Criminal Justice Information Services Division, Logistical Support Unit, 1000 Custer Hollow Road Clarksburg, WV 26306

(2) Questions regarding supplies may be directed to the Logistical Support Unit at (304) 625–3983; orders may be faxed to (304) 625–3984 or submitted electronically at <http://www.fbi.gov/>. All fingerprint-related questions should be directed to USACRC prior to contacting the FBI.

(3) Investigators must ensure that the charges annotated on the FBI Form FD 249 reflect the actual charges being pursued through court-martial or nonjudicial punishment. When submitting the FBI Forms FD 249 and FBI Form R–84, charges must be described in commonly understood descriptive terms (for example, murder, rape, robbery, assault, possession of a controlled substance) or by a commonly understood title. Offenses shall not be described solely by references to a UCMJ punitive article or to the U.S. Code or other statutory provision.

(4) The disposition reflected on the FBI Form FD 249 or the FBI Form R–84 must also be described in common language (for example, conviction (include offense(s)), dishonorable discharge, reduction in rank, forfeiture of pay, charges dismissed). The disposition of “conviction” shall only be reported for crimes prosecuted by general or special court-martial yielding a plea or a finding of guilty.

(a) Adverse findings resulting from a summary court-martial should be recorded as follows: “Subject found guilty by summary court-martial.” Although action by summary courts-martial is disciplinary in nature for a violation of military law, the Supreme Court has ruled that a summary court-martial is not a criminal proceeding in accordance with U.S. Supreme Court Case *Middendorf v. Henry*, 425 U.S. 25 (1976).

(b) Adverse findings resulting from nonjudicial proceedings pursuant to UCMJ, Article 15 will be recorded as “nonjudicial disciplinary action.” An adverse finding or punishment pursuant to UCMJ, Article 15 is a disciplinary action, but does not constitute a criminal proceeding or conviction.

Table 4–1
List of offenses from the Uniform Code of Military Justice

UCMJ article	Offense
78	Accessory after the fact (offenses listed in this table)
80	Attempts (offenses listed in this table)
81	Conspiracy (offenses listed in this table)
82	Solicitation
85	Desertion
90	Striking or assaulting a superior commissioned officer
91	Striking or assaulting warrant, noncommissioned, or petty officer
94	Mutiny or sedition
95	Resistance, breach of arrest, and escape
97	Unlawful detention
106	Spies
106a	Espionage
107	False official statements
108	Military property of the United States, sale, loss, damage, destruction, or wrongful disposition
109	Property other than military property of the United States - waste, spoilage, or destruction
111	Drunken or reckless operation of vehicle, aircraft, or vessel
112a	Wrongful use, possession, etc., of controlled substance
116	Riot or breach of peace
118	Murder
119	Manslaughter
119a	Death or injury of an unborn child
120	Rape and carnal knowledge (for offenses committed prior to October 1, 2007)
120	Rape, sexual assault, and other sexual misconduct (for offenses committed on or after October 1, 2007)
120a	Stalking (for offenses committed on or after October 1, 2007)
121	Larceny and wrongful appropriation
122	Robbery
123	Forgery
123a	Making, drawing, or uttering check, draft, or order without sufficient funds
124	Maiming
125	Sodomy
126	Arson
127	Extortion
128	Assault
129	Burglary
130	Housebreaking
131	Perjury
132	Frauds against the United States
134	Assault—indecent (for offenses committed prior to October 1, 2007)

Table 4-1
List of offenses from the Uniform Code of Military Justice—Continued

UCMJ article	Offense
134	Assault—with intent to commit murder, voluntary manslaughter, rape, robbery, sodomy, arson, burglary, or housebreaking
134	Bribery and graft
134	Burning with intent to defraud
134	Child endangerment (for offenses committed on or after October 1, 2007)
134	Child pornography offenses, to include possession, distribution, production, receipt, viewing, and accessing
134	Correctional custody—offense against
134	False or unauthorized pass offenses
134	False pretenses, obtaining services under
134	False swearing
134	Firearm, discharge—willfully, under such circumstances as to endanger human life
134	Fleeing the scene of an accident
134	Homicide, negligent
134	Impersonating commissioned, warrant, noncommissioned, or petty officer, or an agent or official
134	Indecent acts or liberties with a child (for offenses committed prior to October 1, 2007)
134	Indecent exposure (for offenses committed prior to October 1, 2007)
134	Indecent language
134	Indecent acts with another (for offenses committed prior to October 1, 2007)
134	Kidnapping
134	Mail: taking, opening, secreting, destroying, or stealing
134	Mail: depositing or causing to be deposited obscene matter in
134	Misprision of serious offense
134	Obstructing justice
134	Wrongful interference with an adverse administrative proceeding
134	Pandering and prostitution (Having someone commit an act of prostitution is still an offense pursuant to UCMJ, Article 134, but if the pandering is “compelled” it becomes an offense under UCMJ, Article 120, if on or after October 1, 2007.)
134	Perjury: subornation of
134	Public record: altering, concealing, removing, mutilating, obliterating, or destroying
134	Reckless endangerment
134	Seizure: destruction, removal, or disposal of property to prevent
134	Self-injury without intent to avoid service
134	Soliciting another to commit an offense (for crimes listed in this table)
134	Stolen property: knowingly receiving, buying, concealing
134	Testify: wrongful refusal
134	Threat or hoax designed or intended to cause panic or public fear
134	Threat, communicating
134	Weapon: concealed, carry
134	Any offenses pursuant to 18 USC 13 charged as a violation of UCMJ, Article 134

4-10. Procedures for reporting absence without leave, desertion, and special category absentee offenses

a. Absent without leave reporting procedures.

- (1) The commander will notify the installation PMO or DES of a Soldier’s reported absent without leave (AWOL).
- (2) Upon receipt of an AWOL report, the installation PMO or DES will initiate an LER, and a corresponding information blotter entry.

(3) The PM or DES will following the provisions of AR 190-9 when notification is received that an AWOL or Deserter Soldier has returned to military control or upon apprehension by civilian authorities. The PM/DES will ensure all LERs are updated to reflect the change in status and ensure the unit commander completes the DA Form 4833. If the AWOL Soldier surrenders to the parent unit or is RMC at another installation, the provisions of AR 190-9 will be followed.

b. Desertion reporting procedures.

(1) The commander will report and PMs and DESs will enter a warrant for, desertion for high-risk, a Soldier as a deserter when they depart without authorization, and in the determination of the commander, depart without the intent of returning. This action is also authorized for Soldiers who—without authority—fail to go to, or go from, their appointed place of duty at the time prescribed, and absent themselves with the intent to permanently remain away from their unit, organization, or place of duty; or are classified as a high-risk Soldier. Unit commanders will report the desertion to the PM or DES, who will enter a warrant into NCIC. The issuing of a deserter warrant into NCIC authorizes the Soldier's apprehension or arrest by federal, state, and local law enforcement personnel throughout the United States.

(a) For the purposes of this paragraph, a "high-risk Soldier" is defined in AR 190-9.

(b) When a deserter warrant is being issued based solely on the Soldier's status as "high-risk," the commander will include a written basis (in block 19 of the DD Form 553) for his or her finding that the Soldier is "high-risk." The commander will send a copy of the warrant, on the day it is issued, to the installation SJA for review, to ensure there is a legally justifiable basis for the finding of "high-risk." If the SJA finds the warrant legally insufficient, the warrant will be revoked.

(2) The unit commander must comply with the provisions of AR 630-10 when a Soldier is dropped from the rolls and reported as a deserter.

(3) On receipt of the DD Form 553 (Deserter/Absentee Wanted by the Armed Forces), the installation PMO or DES will—

(a) Initiate an LER and a blotter entry reflecting the Soldier's status as "deserter."

(b) Complete sections of the DD Form 553 concerning the Soldier's driver's license and vehicle information. In the remarks section, add other information known about the Soldier such as: confirmed or suspected drug abuse; history of escape(s) or attempted escape(s) from custody; suicidal tendencies or attempts; use of prescription or other medication(s); involvement in or charge(s) of crimes of violence for which an active military police investigation has been prepared and forwarded; history of unauthorized absences; and any other useful or essential information for the protection of the deserter or apprehending authorities.

(c) Assign the LER number and a USACRC control number, which will be assigned to the case and be included in the remarks section of the DD Form 553.

(d) A copy of the DD Form 553 is sent to USADIP, and the original is sent to the unit commander within 24 hours of receipt.

(4) Complete the special category absentee (SCA) reporting procedures, which are—

(a) Regardless the length of absence, the commander will immediately report a SCA Soldier as a deserter and within 48 hours, notify the installation PMO or DES in writing. Included in this category are defectors, absentee Soldiers who travel to a country other than the one in which they are stationed, and cases in which there is evidence that the Soldier may be involved with a foreign intelligence service or terrorist organization.

(b) The unit commander must comply with the provisions of AR 190-9 and AR 630-10 when reporting a SCA as a deserter.

(c) Upon receipt of the DD Form 553 (Deserter/Absentee Wanted by the Armed Forces), the installation PMO or DES must—

1. Follow desertion reporting procedures in AR 190-9 and AR 630-10.

2. Notify the local supporting counterintelligence office that a SCA has been reported and/or RMC.

3. Notify the Deputy Chief of Staff, G-2 when a defector is RMC.

4-11. Vehicle Registration System

The VRS is a module within COPS. Within VRS there are various tabs for registering vehicles that are authorized access to an installation, to include personal data on the owner of the vehicle. There are also tabs for registering weapons, bicycles, and pets. Information on individuals barred entry to an installation is also maintained within the VRS.

4-12. Establishing memorandums of understanding

a. Coordination between military LE personnel and local civilian LE personnel is essential to improve information sharing, especially concerning investigations, arrests, and prosecutions involving military personnel. The installation PM or DES or other LE officials will establish formal memorandums of understanding (MOUs) with their civilian counterparts to establish or improve the flow of information between their agencies, especially in instances involving military personnel. The MOUs will be used to clarify jurisdictional issues for the investigation of incidents, to define

the mechanism whereby local LE reports involving active-duty Servicemembers will be forwarded to the appropriate installation LE office, to encourage the local LE agency to refer victims of domestic violence to the installation Family Advocacy Office or victim advocate, and to foster cooperation and collaboration between the installation LE agency and local civilian agencies.

b. Installation commanders are authorized, under Section 120(a) of the Water Resources Development Act of 1976, to contract for local, State, or Federal LE services (enforcement of civil and criminal laws of the State) from civilian police departments. Section 120(a) of the Water Resources Development Act of 1976 authorizes the Secretary of the Army, acting through the Chief of Engineers, to contract with States and their political subdivisions for the purpose of obtaining increased law enforcement services at water resource development projects under the jurisdiction of the Secretary of the Army to meet needs during peak visitation periods.

c. The MOUs will address the following issues, at a minimum—

- (1) A general statement of the purpose of the MOU.
- (2) An explanation of jurisdictional issues that affect respective responsibilities to—and investigating incidents occurring on and off—the installation. This section should also address jurisdictional issues when a civilian order of protection is violated on military property (see 10 USC 1561a).
- (3) Procedures for responding to incidents that occur on the installation involving a civilian alleged offender.
- (4) Procedures for local LE to immediately (within 4 hours) notify the installation LE office of incidents and investigations involving Servicemembers.
- (5) Procedures for transmitting incident and investigation reports and other LE information involving active-duty Servicemembers from local civilian LE agencies to the installation LE office.
- (6) Notification of when a Soldier is required to register as a sex offender either through military judicial proceedings or civilian judicial proceedings.
- (7) Procedures for transmitting civilian protection orders (CPOs) issued by civilian courts or magistrates involving active-duty Servicemembers from local LE agencies to the installation LE office.
- (8) Designation of the title of the installation LE recipient of such information from the local LE agency.
- (9) Procedures for transmitting the DD Form 2873 (Military Protective Order) from the installation LE office to the local civilian LE agency with jurisdiction over the area in which the Service member resides.
- (10) Designation of the title of the local LE agency recipient of domestic violence and CPO information from the installation LE agency.
- (11) Respective responsibilities for providing information to victims regarding installation resources when either the victim or the alleged offender is an active duty Service member.
- (12) Sharing of information and facilities during the course of an investigation in accordance with 5 USC 552a(b)(7) (The Privacy Act of 1974).
- (13) Regular meetings between the local civilian LE agency and the installation LE office to review cases and MOU procedures.

4–13. Lost, abandoned, or unclaimed property

Personal property that comes into the possession, custody, or control of the Army and is unclaimed by the owner is considered to be abandoned only after diligent effort has been made to determine and locate its owner, the heir, next of kin, or legal representative. A Soldier who has permanent change of station orders and is unable to dispose of his or her personal property should immediately notify the chain of command. The commander will appoint a board to rule on the disposition of the property. If a LE agency takes custody of the property it will be tagged and a record made as shown in paragraph *a*, below. A report will be made to the installation commander who will take action in accordance with DOD 4160.21–M, chapter 4, paragraph 40. Pending board action under DOD 4160.21–M, the LE agency having physical custody is responsible for the safekeeping of seized property. The following procedures should be used:

- a.* Property will be tagged using DA Form 4002 (Evidence/Property Tag) or clearly identified by other means, inventoried, and made a matter of record. These records are kept by the custodian of the property.
- b.* Lost, abandoned, or unclaimed property will be kept in a room or container separate from one used to store property held as evidence. Records or logs of property not held as evidence will be separated from those pertaining to evidence. However, all property will be tagged, accounted for, and receipted for in a similar manner as evidence.
- c.* Property that has been properly identified through board action under DOD 4160.21–M as having an owner will be segregated and tagged with the name of that person.
- d.* Unclaimed or forfeited property in the custody of the Army will be disposed of by order of any court of record that has territorial jurisdiction over the Army installation.
- e.* A letter will be sent to the owner of the property on the disposition of the property and a memorandum be written indicating that attempts were made to contact the owner of the property which met with negative results and kept on file.
- f.* In all cases, a receipt should be obtained at time of release or disposition.

4-14. Procedures for restricted and unrestricted reporting in sexual assault cases

Active-duty Soldiers, ARNG, and USAR Soldiers who are subject to military jurisdiction under the UCMJ can elect either restricted or unrestricted reporting if they are victims of sexual assault. See AR 600-20 for further details.

- a.* Unrestricted reporting requires normal LE reporting and investigative procedures.
- b.* Restricted reporting requires that LE and criminal investigative organizations not be informed of a victim's identity and not initiate investigative procedures. The victim may provide sexual assault response coordinators (SARCs), medical treatment facility (MTF) personnel, victim advocates, and Sexual Harassment/Assault Response & Prevention Program proponents with specific items (clothing, bedding, and so on) that may later be used as evidence, should they decide later to convert to an unrestricted report. (SARCs and MTF personnel are neither required nor encouraged to collect evidence; however, circumstances may occur where evidence comes into their possession.) In sexual assault cases additional forensic evidence may be collected using the "sexual assault evidence collection kit," (hereafter, "evidence kit"). Personnel from the MTF or SARC releasing evidence to the installation PMO or DES will comply with AR 195-5. The SARC or MTF will have only temporary possession of the evidence and must immediately notify the installation PMO or DES to transfer custody of evidence. The evidence kit, other items such as clothing or bedding sheets, and any other articles provided by the MTF or SARC will be stored in the installation PMO or DES evidence room separate from other evidence and property. The evidence kit, the other items such as clothing or bedding sheets, and any other items will be properly sealed and marked with the restricted reporting control number that is issued by the SARC. Procedures for handling evidence specified in AR 195-5 will be strictly followed.
- c.* The installation PMO or DES will complete an RDF, in the automated DA Form 190-45-SG, also known as ALERTS, for restricted reporting. Reports will be completed using the offense code from the "6Z" series. An entry will be made in the journal when the sexual assault evidence kit or property (clothing, bedding, and so forth) is received. An entry will not be made in the blotter. Restricted reporting incidents are not reportable as SIRs. Property will be stored for 5 years and then scheduled for destruction, unless previously released to investigative authorities. Thirty days prior to destruction of the property, a letter will be sent to the SARC by the installation PMO or DES, advising the SARC that the property will be destroyed in 30 days, unless LE personnel are notified by the SARC that the victim has elected unrestricted reporting. If the SARC notifies the installation PM or DES that the victim has not elected unrestricted reporting, clothing, or other personal effects will be released to the SARC for return to the victim. The information report will be updated when the evidence is destroyed, returned to the SARC, or released to investigative authorities.
- d.* In the event that information about a sexual assault that was made under restricted reporting is disclosed to the commander from a source independent of the restricted reporting avenues, or to LE from other sources, the commander will report the matter to LE. In this situation, LE remains authorized to initiate its own independent investigation of the matter presented. Additionally, a victim's disclosure of his or her sexual assault to persons outside the protective sphere of those covered by the restricted reporting policy will result in an investigation of the allegations.

4-15. Procedures for restricted and unrestricted reporting in domestic violence cases

Restricted reporting is a reporting option for adult victims of domestic abuse. For the purposes of this paragraph, restricted reporting is defined as allowing a victim of domestic abuse, who is eligible to receive military medical treatment, including civilians and contractors who are eligible to receive military healthcare OCONUS on a reimbursable basis, the option of reporting an incident of domestic abuse to specified individuals without initiating the investigative process or notification to the victims or the alleged offender's commander. For the purposes of this paragraph, an adult is a Soldier or a person who is not a Soldier who has either attained the age of 18 years of age or is married.

- a.* Unrestricted reporting requires normal LE reporting and investigative procedures.
- b.* Restricted reporting requires that LE and criminal investigative organizations not be informed of a victim's identity and not initiate investigative procedures. The victim will provide the victim advocate or MTF personnel with specific items that will be later used as evidence, should they decide to later report the incident to LE. Victim advocates and MTF personnel are neither required nor encouraged to collect evidence; however, circumstances will occur where evidence comes into their possession. Victim advocates and MTF personnel will have only temporary possession of the evidence and must immediately notify the installation PMO or DES to transfer custody of evidence. These items will be stored in the installation PMO or DES's evidence room separate from other evidence and property. Procedures for handling evidence specified in AR 195-5 will be strictly followed.
- c.* The installation PMO or DES will complete an RDF in DA Form 190-45-SG, also known as ALERTS, for domestic violence restricted reporting. Reports will be completed using the offense code from the "9U" series. An entry will be made in the journal when the property is received. An entry will not be made in the blotter. Restricted reporting incidents are not reportable as SIRs. Property will be stored for 1 year and then scheduled for destruction, unless previously released to investigative authorities. Thirty days prior to destruction of the property, a letter will be sent to the family advocacy program manager and the victim advocate by the installation PMO or DES, advising the victim advocate that the property will be destroyed in 30 days, unless LE personnel are notified by the victim advocate that the victim has elected unrestricted reporting. The information report will be updated when the evidence is destroyed or released to investigative authorities.

d. A victim's disclosure of his or her domestic violence incident to persons outside the protective sphere could result in an investigation of the allegations.

4-16. Domestic violence

a. Responding to incidents of domestic violence requires a coordinated effort by LE, medical, and social work personnel, to include sharing information and records as permitted by law and regulation. AR 608-18 contains additional information about domestic violence and protective orders. AR 608-18's glossary refers to domestic violence as including the use, attempted use, or threatened use of force or violence against a person or a violation of a lawful order issued for the protection of a person, who is (a) a current or former spouse; (b) a person with whom the abuser shares a child in common; or (c) a current or former intimate partner with whom the abuser shares or has shared a common domicile."

b. All domestic violence incidents will be reported to the local installation PMO or DES. All reported domestic violence incidents will be entered into MPRS, using the LER. These codes will be used in addition to any other offense code that is appropriate for an incident. For example, a Soldier strikes his or her spouse. When entering the offense data into DA Form 190-45-SG, also known as ALERTS, both the offense code for assault (that is, 5C2) and the offense code for spouse abuse (from the 9UI series) will be entered.

4-17. Protection orders

a. *Documentation.* A DD Form 2873 (Military Protective Order) is a written lawful order issued by a commander that orders a Soldier to avoid contact with those persons identified in the order. DD Forms 2873 may be used to facilitate a "cooling-off" period following domestic violence and sexual assault incidents, to include incidents involving children. The commander should provide a written copy of the order within 24 hours of its issuance to the person with whom the member is ordered not to have contact and the installation LE activity. A reply by endorsement can be completed for the pertaining LER, indicating that a DD Form 2873 has been issued. Violations of a DD Form 2873 must be reported on the LER and entered into DA Form 190-45-SG, also known as ALERTS. All protective orders will be entered into DA Form 190-45-SG, also known as ALERTS, and the NCIC system. Violations of a DD Form 2873 likely constitute violations of Article 90 or 92, UCMJ.

(1) *Initial notification.* In the event a DD Form 2873 is issued against a Soldier and any individual involved in the order does not reside on an Army installation at any time during the duration of the DD Form 2873, the installation PMO or DES will notify the appropriate civilian authorities (local magistrate courts, family courts, and local police) of—

- (a) The issuance of the protective order.
- (b) The individuals involved in the order.
- (c) Any change made in a protective order.
- (d) The termination of the protective order.

(2) *Civilian-authority notification.* The installation PMO or DES will notify the appropriate civilian authorities (local magistrate courts, family courts, and local police) of the protective order. The installation PMOs and DESs will place the DD Forms 2873 in the NCIC Protective Order File, along with civilian protective orders. This provides the electronic means for military commanders to make information on the issuance of a DD Form 2873 available to all civilian law enforcement authorities.

(a) The DES or PMO will place the active DD Form 2873 in NCIC for the duration of the order. The DES or PMO will initiate an LER for the DD Form 2873, creating the required originating agency case number, and place the DD Form 2873 in the NCIC POF, using "Protection Order Conditions Field Code 08" with the following mandatory caveat in the miscellaneous field: "This is a Military Protective Order and may not be enforceable by non-military authorities. If subject is in possible violation of the order, advise the entering agency (Military Law Enforcement)."

(b) Updating and termination of a DD Form 2873 in NCIC will follow normal NCIC operational procedures. Installation law enforcement will further notify surrounding civilian law enforcement jurisdictions of the DD Form 2873 submission via an NCIC administrative message.

b. *Compliance.* A CPO is an order issued by a judge, magistrate or other authorized civilian official, ordering an individual to avoid contact with his or her spouse or children. Pursuant to Section 1561a, Title 10, United States Code (The Armed Forces Domestic Security Act) a CPO has the same force and effect on a military installation as such order has within the jurisdiction of the court that issued the order. LE personnel will complete an LER, in DA Form 190-45-SG, also known as ALERTS, whenever a CPO is issued that orders a Soldier to avoid contact with his or her spouse or children or orders an individual to avoid contact with his or her military spouse or Family members. Violations of a CPO must be reported on the LER and entered into DA Form 190-45-SG, also known as ALERTS.

4-18. Defense Incident-Based Reporting System/National Incident-Based Reporting System reporting responsibilities

a. Reporting processes involve several databases that rely on shared information.

(1) DA Form 190–45–SG, also known as ALERTS, consolidates and forwards monthly DIBRS reports to Defense Manpower Data Center.

(2) The DIBRS reporting process will be triggered when law enforcement officials respond to a founded offense of a criminal incident. The LE officials will collect information necessary to fulfill reporting responsibilities by filling out the LER. The installation PMO or DES must ensure cases in DA Form 190–45–SG, also known as ALERTS, are changed from “open” or “final” status to “closed” to ensure that the LER is reported to DIBRS. If the crime is determined to be outside the jurisdiction of the LE organization, the DIBRS reporting responsibility will be passed to the appropriate agency, such as USACIDC, the FBI, or the local authority that has accepted investigative jurisdiction of the case.

b. If the investigation is initiated by or referred to USACIDC and USACIDC assumes the lead investigative role, it also assumes DIBRS reporting responsibility.

c. Army LE agencies will normally refer cases involving military offenders to the responsible commander for appropriate action. The responsible LE agency will initiate the LER. The commander may refer the case to staff agencies, dispose of the case pursuant to administrative or nonjudicial authority, or refer the case to court-martial or to an appropriate convening authority for ultimate disposition. The commander taking final action on the case will forward the DA Form 4833 to the local installation PMO or DES. If the case is forwarded to another convening authority for action, the commander assuming jurisdiction over the case is responsible for forwarding the DA Form 4833 to the local installation PMO or DES.

d. In some instances, commanders will be required to initiate DIBRS reporting when a military law enforcement activity is not involved. Commanders will ensure that reporting responsibilities and requirements as prescribed in this policy are met in these cases, and a DA Form 4833 is submitted to the local installation PMO or DES.

e. SJAs will forward all supporting judicial documents to the commander. The commander will attach the DA Form 4833 and send to the local installation PMO or DES within the prescribed 60 days.

f. Regarding reporting requirements, an incident that is listed in table 4–1 will be reported on an LER or ROI if initiated by LE. If a commander initiates reporting an incident, it will be documented and submitted on a DA Form 4833 with supporting documents (UCMJ, Article 15 court reports) and submitted to the installation PM or DES. Reportable incidents include:

(1) Criminal incidents not listed in table 4–1, but punishable under the UCMJ. This includes incidents such as fraternization, sexual harassment, sexual assault, and rape.

(2) Civilian criminal incidents committed by military personnel on active duty resulting in a felony conviction, as defined in the civilian jurisdiction where the offense is tried.

g. Other reportable incidents include:

(1) Sudden infant death syndrome when the victim is a dependent residing with an active-duty Servicemember.

(2) Incidents involving the actual or attempted suicide of military personnel on active duty.

(3) Other incidents requiring action under 18 USC 922 (The Brady Handgun Violence Prevention Act of 1993, Revised Statute).

(4) Incidents covered by Public Law No. 97–291, Volume 96, US Statute at Large 1248 (Victim and Witness Protection Act of 1982) codified as amended in scattered sections of 18 USC and the Federal Rules of Criminal Procedure 32(c)(2). Army LE authorities must advise the victim or witness of their rights using the DD Form 2701 (Initial Information for Victims and Witnesses of Crime) in accordance with chapter 6 of this regulation. Victim-witness notifications will be reported on the LER to provide accountability in the automated DA Form 190–45–SG, also known as ALERTS.

(5) Commanders and family-advocacy programs will report all domestic violence incidents to the local installation PMO, DES, or CID office which includes:

(a) Incidents that involve evidence determined sufficient for supporting disciplinary action and, for each such incident, a description of the allegations and the action taken by command authorities in the incident.

(b) Incidents that involve evidence determined insufficient for supporting disciplinary action and, for each such case, a description of the allegation.

Chapter 5

Army Law Enforcement Trends and Analysis Report

5–1. General

a. This chapter prescribes policies and procedures for the coordination and standardization of crime statistics reporting with HQDA. Crime statistical reports and trends provided to HQDA and other agencies and those related to special interests inquiries, the media, and the public must reflect uniformity in terminology, methods of presentation, and statistical portrayal to preclude misinterpretation of information.

b. Any report containing Armywide aggregate crime data or statistics addressed to the Secretary of the Army, Chief

of Staff of the Army, or Vice Chief of Staff of the Army will be coordinated and cleared with HQDA, OPMG (DAPM–MPO–LE). Correspondence and reports will be coordinated with HQDA, OPMG (DAPM–MPO–LE) prior to release to any agency, activity, or individual.

c. HQDA staff agencies and ACOMs, ASCCs, and DRUs authorized by regulation or statute to conduct independent investigations, audits, analyses, or inquiries need not coordinate reported information with HQDA, OPMG (DAPM–MPO–LE) unless the information contains crime data for the Army as a whole. For example, reports submitted by USACIDC containing only USACIDC investigative data need not be coordinated with HQDA, OPMG (DAPM–MPO–LE).

5–2. Crime rate reporting

a. The USACIDC, Command Intelligence Operation Center (CIOC) develops criminal intelligence through the collection of raw criminal information and the centralized analysis of crime cases and other related data. The USACIDC analyzes and identifies modus operandi, trends, and vulnerabilities, and disseminates this information to DOD, Army LE and investigative agencies.

b. The CIOC criminal intelligence (CRIMINTEL) analyst provides in-depth analysis addressing current and future criminal trends and force-protection threats affecting Army installations worldwide. Army aggregate crime reports include data accessible through DA Form 190–45–SG, also known as ALERTS, and other available DOD databases.

Chapter 6

Victim and Witness Assistance Procedures

6–1. General

a. This chapter implements procedures to provide assistance to victims and witnesses of crimes that take place on Army installations and activities. The procedures in this chapter apply to—

- (1) Every victim and witness.
- (2) Violations of the UCMJ, including crimes assimilated under the Assimilative Crimes Act reported to, or investigated by, Army LE.
- (3) Foreign nationals employed or visiting on an Army installation OCONUS.

b. Installation PM or DES personnel should refer to AR 27–10 for additional policy guidance on the Army Victim/Witness Program.

6–2. Procedures

a. As required by DODD 1030.1, Army personnel involved in the detection, investigation, and prosecution of crimes must ensure that victim and witness rights are protected. Victims' rights include—

- (1) The right to be treated with fairness, dignity, and a respect for privacy.
- (2) The right to be reasonably protected from the accused offender.
- (3) The right to be notified of court proceedings.
- (4) The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial, or for other good cause.
- (5) The right to confer with the attorney for the Government in the case.
- (6) The right to restitution, if appropriate.
- (7) The right to information regarding conviction, sentencing, imprisonment, and release of the offender from custody.

b. In keeping with the requirements listed above, the installation PM or DES must ensure that—

- (1) All LE personnel are provided copies of DD Form 2701 (Initial Information for Victims and Witnesses of Crime).
- (2) A victim and witness coordinator is appointed in writing.
- (3) Statistics are collected and reported into DA Form 190–45–SG, also known as ALERTS.
- (4) Coordination with the installation SJA victim/witness coordinator occurs to ensure that individuals are properly referred for information on restitution, administrative, and judicial proceedings.
- (5) Coordination with installation Family Advocacy Program's victim advocate occurs to support victims of domestic abuse. Victim advocacy services include crisis intervention, assistance in securing medical treatment for injuries, information on legal rights and proceedings, and referral to military and civilian shelters and other resources available to victims.

6-3. Notification

a. LE personnel will provide crime victims and witnesses a DD Form 2701, and ensure that individuals are notified about—

- (1) Available military and civilian emergency medical care.
- (2) Social services, when necessary.
- (3) Procedures to contact the SJA victim/witness liaison office for additional assistance.

b. Investigating LE personnel, such as Army LE investigators will—

- (1) Ensure that victims and witnesses have been offered a DD Form 2701. If not, investigating personnel will give the individual a copy.
- (2) Provide status on investigation of the crime to the extent that releasing such information does not jeopardize the investigation in coordination with the installation PM or DES victim and witness coordinator.
- (3) Inform all victims and witnesses of the apprehension of a suspected offender, if requested.

6-4. Statistical reporting requirements

a. The DOD policies on victim and witness assistance require reporting of statistics on the number of individuals who are notified of their rights. The LER provides for the collection of statistical information.

b. The DA Form 190-45-SG, also known as ALERTS, supports automated reporting of statistics. HQDA PMG (DAPM-MPO-LE), as the program manager, will require periodic reports to meet unique requests for information.

c. It is possible that a victim or witness will initially decline a DD Form 2701. As the case progresses, the individual will request information. If a case is still open, the PM or DES victim and witness coordinator will provide the DD Form 2701 (Initial Information for Victims and Witnesses of Crime) to the individual and update the records. Once the case is referred to the SJA, or LE activity ceases, DA Form 190-45-SG, also known as ALERTS, will not be updated without prior coordination with the installation SJA Office.

Chapter 7 Related Military Police Forms

7-1. General

a. This chapter establishes policies and procedures for the use of related MP forms. Other forms are referenced in this chapter to assist in meeting LE requirements.

b. It also provides special instructions and distribution for each related form listed in chapter 7 of this publication, and prescribes accountability standards for DD Form 1408 (Armed Forces Traffic Ticket) and the Central Violations Bureau Form.

7-2. DD Form 460 (Provisional Pass)

a. *General.* DD Form 460 will be used by the installation PM or DES to permit members of the U.S. Armed Forces to travel to assigned units under the following conditions:

- (1) A person is apprehended for a violation not serious enough to warrant further custody, but the person is delayed to the extent that reporting to the assigned station within the time limit of existing orders is not possible.
- (2) An absentee is returned to military control and an escort is not considered necessary in returning the Soldier to the unit of assignment.
- (3) A Soldier's leave papers have been lost or destroyed.
- (4) A Soldier is about to exceed the limits of an authorized leave or travel order.

b. *Special instructions.*

- (1) The form is self-explanatory. Signature authorities will be prescribed by local policy.
- (2) Refer to AR 190-9 and AR 630-10 for guidance on use of DD Form 460 in the AWOL and Deserter Apprehension Program.

c. *Distribution.*

- (1) The original copy is provided to the individual.
- (2) The first copy (green) is attached to the file copy of the LER.
- (3) The second copy (yellow) is attached to the action or RDF, which is forwarded to the commander concerned.

7-3. DD Form 553 (Deserter/Absentee Wanted by the Armed Forces)

a. *General.* DD Form 553 is used to—

- (1) Provide the unit commander a means of reporting cases of desertion to the USADIP and to the local PM or DES.
- (2) Provide USADIP a means of requesting deserter apprehension assistance from Federal, State, and local law-enforcement authorities.

b. Special instructions. The provisions of AR 630–10 and AR 190–9 must be reviewed and applied to each desertion case. AR 630–10 contains personnel management procedures that must be followed, and AR 190–9 provides policy guidance on law-enforcement procedures.

c. Distribution.

- (1) Unit commanders will provide the original and one copy of DD Form 553 to the installation PM or DES.
- (2) The installation PM or DES will comply with AR 630–10 and AR 190–9.
- (3) Until the deserter is returned to military control, USADIP will maintain the active file.

7–4. DD Form 616 (Report of Return of Absentee)

a. General. DD Form 616 is used to advise USADIP, the installation PM or DES, and civil authorities of the return to military control of persons previously reported as deserters and to cancel DD Form 553 entered into the NCIC.

b. Special instructions. When a deserter is returned to military control, the installation PM or DES will complete the DD Form 616, per paragraph 4–11 of this regulation, and the provisions of AR 190–9.

c. Distribution.

(1) The installation PM or DES receiving custody of a deserter will forward one copy of the DD Form 616 to USADIP and retain one copy in the inactive deserter file.

(2) The PM or DES of other installations who received DD Form 553 from USADIP will retain a copy of DD Form 616 with the DD Form 553 in the inactive deserter file.

7–5. DD Form 2708 (Receipt for Pre Trial/Post Trial Prisoner or Detained Person)

a. General. DD Form 2708 is used to transfer custody of prisoners or apprehended persons who cannot be released on their own recognizance.

b. Special instructions. For law enforcement purposes, the form is self-explanatory. For confinement facility personnel, see AR 190–47.

c. Distribution.

(1) The original is attached to the file copy of the LER.

(2) A second copy is provided to the individual receiving custody.

7–6. DD Form 1408 (Armed Forces Traffic Ticket)

a. General. DD Form 1408 is used to report minor traffic violations not reported on the Central Violations Bureau Form or the LER.

b. Special instructions.

(1) A Privacy Act Statement will be required to obtain an individual's SSN. Chapter 2 of this regulation provides additional guidance.

(2) The front side will be prepared by the issuing law enforcement official.

(3) The rear of the yellow and pink copy is also prepared by the issuing LE official.

(4) The issuing installation PM or DES will complete the rear of the white copy, to include the date, name, organization, "to" and "from" blocks, and will assign a suspense date.

(5) The receiving commander will complete the remainder of the rear of the white copy and return the form to the installation PM or DES.

(6) DD Form 1408 may be used as a warning notice. The warning block will be checked and the reason for the warning will be cited in the remarks section.

c. Distribution.

(1) The original (white copy) will be forwarded through local distribution to the commander concerned.

(2) The second copy (yellow) will be filed by the issuing installation PM or DES until the original is returned.

(3) The third copy (pink) will be presented to the violator.

7–7. United States District Court Central Violations Bureau Form

a. General. The Central Violations Bureau Form is an accountable form prepared by LE personnel to report minor offenses to include violations of state traffic laws applicable to military reservations. This form is used only in conjunction with a magistrate court system. When used to cite military and DOD-affiliated personnel for violations that are normally processed by mail, the appropriate commander will be informed. An information LER, denoting in the appropriate blocks the date, time, place, and type of violation will be used to transmit a copy of the Central Violations Bureau Form to the commander or supervisor. The amount of money subject to forfeiture should also be included. Local policy will determine which offenses are reported to the district court or U.S. Magistrate.

b. Special instructions.

(1) A Privacy Act Statement will be required to obtain an individual's SSN. Chapter 2 of this regulation provides additional guidance.

(2) The installation PM or DES must maintain liaison with the local U.S. Magistrate to determine accountability of

the form and the referral of charges. The provisions of chapter 4 of this regulation provide guidance on reporting offenses that will involve the use of the Central Violations Bureau Form.

c. Distribution. Distribution of the form will comply with chapter 4 of this regulation and the instructions printed on the form.

7-8. DD Form 1920 (Alcohol Incident Report)

a. General. DD Form 1920 is used to record the condition and behavior of individuals apprehended for offenses in which alcoholic or drug influence is a factor.

b. Special instructions. This form will be prepared for all offenses in which alcohol or drug is considered to have been a factor.

c. Distribution. DD Form 1920 will be an enclosure to the LER.

7-9. DA Form 2804 (Crime Records Data Reference)

a. General. DA Form 2804 (Crime Records Data Reference) is used to provide identifying information on subjects of LERs to USACRC.

b. Special instructions. One completed form will be submitted for each offender.

c. Distribution.

(1) The original is forwarded with the LER to the USACRC.

(2) If a supplement LER is prepared, a DA Form 2804 will be completed and submitted to the Director, USACRC. This is especially important when a report's status is changed from founded to unfounded.

(3) The original is forwarded, with the LER, to the USACRC.

(4) The copy is filed with the corresponding LER by the installation PM or DES initiating the form.

7-10. DA Form 2823 (Sworn Statement)

a. General. DA Form 2823 is used to record written statements of all persons related to reported incidents.

b. Special instructions. DA Form 3881 (Rights Warning Procedure/Waiver Certificate) must be prepared before a sworn statement is taken from a subject or suspect (see para 7-11).

c. Distribution. One copy of the statement will be attached to each copy of the related LER.

7-11. DA Form 3881 (Rights Warning Procedure/Waiver Certificate)

a. General. DA Form 3881 is used to provide a standardized, legally sufficient, narrative rights warning for suspects or subjects.

b. Special instructions. This form must accompany a DA Form 2823 when the individual is a subject or suspect of an LER.

c. Distribution. The DA Form 3881 must accompany each copy of the DA Form 2823. If a subject declines to be questioned, resulting in no DA Form 2823 being prepared, a copy of the DA Form 3881 will accompany each copy of the LER.

7-12. DA Form 3626 (Vehicle Registration/Driver Record)

a. General. DA Form 3626 will be used to—

(1) Provide privately owned vehicle registration information for installations with a vehicle registration program.

(2) Record traffic violation data on persons operating motor vehicles on Army installations.

b. Special instructions. See AR 190-5 for complete instructions and administration of the traffic point system.

c. Distribution. See AR 190-5.

7-13. DA Form 3945 (Military Police Radio Log)

a. General. DA Form 3945 is used to record official Army LE radio transmissions not recorded by electronic means.

b. Special instructions. This form is generally used as a 24-hour record of Army LE radio traffic reflecting patrol dispatches and calls for service.

c. Distribution. No copies are required. The original is filed chronologically at the installation PMO or DES.

7-14. DA Form 3946 (Military Police Traffic Accident Report)

a. General. DA Form 3946 is used to record details of motor vehicle traffic accidents.

b. Special instructions.

(1) A Privacy Act Statement will be required (see chap 2).

(2) General instructions for completion of the form are included with the form.

c. Distribution.

(1) The LER is the transmittal document.

(2) The original DA Form 3946 is forwarded to the applicable commander.

- (3) A copy is retained in the installation files of the PM or DES.
- (4) When appropriate, the original will be attached to the original LER and sent to USACRC. In such cases, the first copy will be retained by the installation PM or DES, and a reproduced copy will be sent to the commander.
- (5) A copy will be provided to the installation safety office on accidents reported or investigated by MP which resulted in a fatality, personal injury, or estimated damage to Government property or privately owned vehicle in excess of \$1,000.

7-15. The blotter report

a. General. The blotter report provides a chronological record of Army LE activities developed from reports, complaints, information incidents, and related events. The RDF from DA Form 190-45-SG, also known as ALERTS, provides a chronological record output suitable for electronic transmission or print on plain paper when needed. All installations are required to use DA Form 190-45-SG, also known as ALERTS, to generate the blotter report. This is the only authorized form used to record LE activities.

b. Special instructions.

(1) Entries will not include the names of juvenile subjects, their parents, guardians, or sponsors. Entries will not list the name of any victim of sensitive incidents (for example, rape). When legitimate LE requirements are met, the term “protected identity” (PI) will be entered where the name, SSN, and address are normally listed.

(2) The term “Restricted Entry” will replace the entire blotter entry for cases in which information concerning the matter should be controlled. Examples of restricted cases include all types of sex-related offenses and other cases deemed appropriate by local policy. Use of restricted entry is authorized to protect information related to on-going police investigations, when publication could adversely impact the investigation or endanger the lives of LE personnel or informants. The responsibility to provide timely and accurate information to commanders, the chain of command, and HQDA will be considered when entering names of subjects.

(3) The first page of the complete blotter and all extracts will include the following statement: “This blotter (or blotter extract) is a daily chronological record of police activity developed from reports, complaints, incidents, or information received, and actions resulting therefrom. Entries contained in the blotter will not be completely accurate and are not adjudications attesting to the guilt or innocence of any person.” Blotters will be stamped “FOUO.” Separate blotter pages or attachments containing protected identity entries will be filed with juvenile records.

c. Distribution. A complete blotter will generally be provided to the senior supported commander, SJA, and USACIDC. Installation information security managers will be authorized by the commander to review the entire blotter for the purpose of submitting derogatory information reports to the Central Clearance Facility. Distribution of redacted blotter entries should be limited to commanders or civilian supervisors of personnel who are the subjects or victims of a crime or accident. Supported commanders will also direct distribution of extracts to staff activities with responsibility for direct support to personnel involved in specified categories of crime or incidents. Examples would be distribution of traffic accident information to the safety officer; distribution of domestic violence reports to the social work services counselor; or alcohol related crimes to the ASAP manager.

7-16. DA Form 4002 (Evidence/Property Tag)

a. General. DA Form 4002 is used to identify property seized as evidence or held for safekeeping.

b. Special instructions. This form should remain attached to the property until final disposition has been determined.

c. Distribution. None.

7-17. DA Form 4137 (Evidence/Property Custody Document)

a. General. DA Form 4137 is used to maintain a chain of custody on seized, impounded, or retained property passed from one individual to another. This form is also used to record found property recovered by the Army LE.

b. Special instructions.

(1) See AR 195-5 for further guidance.

(2) The original will remain in the installation PMO’s or DES’ evidence room, or lost-and-found files, until final disposition of the related case.

c. Distribution.

(1) The original and first copy will remain attached to the property.

(2) The second copy will be attached to the related LER.

(3) The third copy to the person releasing the property.

(4) The original will be filed with the LER, when property not processed through the evidence or lost and found property room is released.

7-18. Accountability of DD Form 1408 and the Central Violations Bureau Form

DD Form 1408 and the Central Violations Bureau Form are accountable forms. The installation PM or DES will establish an accounting system to control these forms. An audit trail will be maintained from issue, to use, and eventual

filing. All forms must be accounted for, including voided forms. Local policy will determine procedures for voiding forms and investigating missing forms.

Chapter 8

Reportable Serious Incidents

8-1. Policy

a. Reports submitted according to this regulation are LE reports in accordance with AR 25-55. Incidents listed in paragraphs 8-2 and 8-3 of this regulation, are reportable to HQDA through PM or DES channels as category 1 and 2 serious incidents, respectively. The lists are not all inclusive. Commanders should report any incident that might concern HQDA as a serious incident, regardless of whether it is specifically listed in paragraphs 8-2 and 8-3. In cases of doubt, report the incident. In determining whether an incident is of concern to HQDA, the following factors should be considered:

- (1) Severity of the incident.
- (2) Potential for adverse publicity.
- (3) Potential consequences of the incident.
- (4) Whether or not the incident is reportable under other reporting systems.
- (5) Effect of the incident on readiness or the perception of readiness.

b. Submission of an SIR will not be delayed due to incomplete information. All pertinent information known at the time of SIR submission will be included. Additional required information will be provided in a subsequent add-on report.

c. Commands that do not have an installation PM or DES will ensure that SIRs are reported to the installation PMO or DES that has geographical LE responsibility for that particular area (see table 1-1 of this regulation). The installation PM or DES will be responsible for initial and follow-on SIR and for the initiation of the LER, for reportable offenses. ACOMs that have off-post activities or facilities are required to immediately notify their installation PM or DES with geographic responsibility for the area of any SIR qualifying events that occur at the activity or facility. The installation PM or DES will be responsible for initial and follow-on SIR reporting.

d. Incidents listed in paragraphs 8-2 and 8-3, occurring on Army installations and facilities are clearly reportable. Commanders should consider the degree of Army interest and involvement in deciding to report incidents occurring off the installation. Any incident where a Soldier is the subject or victim of a serious incident is reportable no matter where it occurs. An incident involving a command-sponsored Family member or DA civilian employee OCONUS is also reportable. Incidents where a Family member, or DA civilian employee, is the subject or victim of a similar incident off post in the United States is not reportable, absent other connections to the Army.

e. On occasion, HQDA, OPMG will direct reporting of incidents or crimes that are not normally reportable. In these instances, the commanders of IMCOM regions, ACOMs, ASCCs, DRUs, and installations will be notified by message of specific requirements and time periods for reporting.

f. All SIRs in which a Soldier is listed as a subject will state whether the Soldier has deployed within the past year.

g. The Army's policy regarding the release of protected health information to LE officials for LE purposes mirrors the policy found in DOD 6025.18-R, paragraph C7.6.

h. In addition to SIR reporting, the incidents described below in paragraphs 8-2*c* and *d*, and any other matters of CI interest as specified in AR 381-12, will be reported to the nearest Army CI office.

i. Commanders and directors of biological select agents and toxins (BSAT) facilities will report as a category 1 SIR, an actual or alleged BSAT incident. The category 1 SIR will be reported by telephone to the Army Watch (DSN 225-4695/96) immediately upon discovery or notification at the installation level. The telephonic report will be followed by a written report, preferably by electronic mail to the ArmyWatch at: usarmy.pentagon-e.hqda.mbx.armywatch@mail.mil within 12 hours of discovery or notification.

8-2. Category 1 reportable serious incidents

These are actual or alleged incidents involving the following:

a. On- and off-post riots, serious disturbances, or demonstrations targeted against the Army or involving Army personnel.

b. War crimes, including mistreatment of enemy prisoners of war, detainees, displaced persons, retained persons, or civilian internees; violations of the Geneva Conventions; and atrocities.

c. Requests by members of the Army for political asylum in foreign countries or indications of defection.

d. Terrorist activities, sabotage, and incidents, initiated or sponsored by known terrorists, dissident groups, or criminal elements that occur on an installation or that involve military personnel or property off an installation.

e. Bomb or explosive incidents resulting in death, injury of military personnel, or damage to military property.

f. Incidents involving material damage that seriously degrade unit operational or training readiness.

g. Threats against Government weapons and ammunition.

h. Information on threats, plans, or attempts to harm or kidnap, or other information bearing on the personal security of the President of the United States, Vice President of the United States, or other persons under U.S. Secret Service (USSS) protection.

i. Incidents involving Army BSAT listed below will be reported. The list of select agents is reviewed and updated by the Centers of Disease Control and Prevention and the Animal and Plant Health Inspection Service and is found in 42 CFR 73; 7 CFR 331; and 9 CFR 121. These agents are also known as high-consequence, nonoverlap agents and toxins; overlap agents and toxins; and listed plant pathogens. The list includes specific genetic elements, recombinant nucleic acids, and recombinant organisms. The list also identifies exclusions—things that are not considered as select agents or toxins (see <http://www.cdc.gov/od/sap/docs/salist.pdf>).

(1) The theft, loss, recovery, suspected theft, inventory shortage or overage, wrongful disposition, and unauthorized use and/or destruction of Army-owned BSAT.

(2) Attempts to steal or divert Army BSAT outside of physical security controls.

(3) Actual or attempted housebreaking or unauthorized access at an Army BSAT facility or laboratory.

(4) Actual or attempted housebreaking or unauthorized access at an off-post BSAT facility or laboratory under contract to the U.S. Army for BSAT research.

(5) Significant or disabling damage to an Army-owned BSAT facility.

(6) Discharge of a select agent or toxin external to the containment laboratory and into the ambient air or environment.

(7) Mishaps in which there was direct evidence of an exposure to Army-owned BSAT, such as a measurable rise in specific antibody strength to the causal agent in question, or a confirmed diagnosis of intoxication or disease.

(8) Other incidents at Army-owned BSAT facilities not identified above that the commander determines to be of immediate concern to HQDA based on the nature, gravity, and potential for adverse publicity, or potential consequences of the incident.

j. Incidents involving Army chemical agents, or research chemical agents, listed below will be reported:

(1) The theft, loss, recovery, suspected theft, inventory shortage or overage, wrongful disposition, and unauthorized use and/or destruction of Army chemical agents or Army research chemical agent.

(2) Attempts to steal or divert Army chemical agents or Army research chemicals outside of physical security controls.

(3) Actual or attempted housebreaking, or unauthorized access at an Army chemical facility or laboratory.

(4) Actual or attempted housebreaking, or unauthorized access at an off-post chemical facility or laboratory under contract to the U.S. Army for chemical research.

(5) Significant or disabling damage to an Army chemical facility.

(6) Mishaps that result in observable or known occupational exposures to Army chemical agents due to failure of personal protective equipment (PPE) to provide protection (such as malfunctions, improper, or inadequate use of PPE).

(7) Other Army chemical or Army research chemical agent incidents not identified above that the commander determines to be of immediate concern to HQDA based upon the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

(8) Any other incident the commander determines to be of immediate concern to HQDA based on the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

8-3. Category 2 reportable serious incidents

These are actual or alleged incidents involving the following:

a. Theft, suspected theft, wrongful appropriation, or willful destruction of Government property or appropriated funds valued at more than \$100,000.

b. Theft, suspected theft, negligence, or conflict of interest involving Government nonappropriated funds or property valued at more than \$100,000.

c. Racially or ethnically motivated criminal acts.

d. Loss, theft, wrongful disposition, willful destruction, or mismanagement of the following:

(1) Evidence as part of a law enforcement investigation.

(2) Sensitive items, other than arms and ammunition, identified by controlled inventory item code 1-6, 8, 9, Q, R, or Y (see AR 710-2).

(3) Controlled cryptographic items.

(4) Drugs identified in 21 USC 13 (The Comprehensive Drug Abuse Prevention and Control Act of 1970) as schedules 1, 2, 3, 4, and 5 controlled substances. Schedules 2 through 5 drugs are Government-controlled medical substances and are identified as R and Q, controlled, medical items in the Federal Supply Catalog. Schedule I drugs, as identified in the act, are only used by DOD for research, and are not available through the supply system.

e. Wrongful possession, manufacture, or distribution of controlled substances, to include narcotics, drugs, or marijuana in the quantities listed below:

- (1) Cocaine, 100 grams or more.
 - (2) Marijuana, 1000 grams or more.
 - (3) Hashish, 1000 grams or more.
 - (4) Heroin, 100 grams or more.
 - (5) Methamphetamines or barbiturates, 100 grams or more.
 - (6) LSD, 6 dosage units or more.
 - (7) PCP, 100 grams or more.
 - (8) For narcotics and dangerous drugs not listed, use quantities for like substances listed above.
- f.* Significant violations of Army standards of conduct, to include bribery, conflict of interest, *Middendorf v. Henry*, or acceptance of gratuities by Soldiers or DA or nonappropriated fund employees.
- g.* Incidents involving prisoners or detainees of Army confinement or correctional facilities to include escape from confinement or custody, disturbances which require the use of force, wounding, or serious injury to a prisoner, and all prisoner deaths.
- h.* Theft, loss, suspected theft, unaccounted or recovered arms, ammunition, and explosives (AA&E) in the following quantities:
- (1) Any missile, rocket, mine, artillery, or mortar rounds.
 - (2) Any machinegun or automatic-fire weapon.
 - (3) Any fragmentation, concussion, high-explosive grenade, or other type of simulator or device containing explosive materials, including artillery or ground burst simulators.
 - (4) Any explosives, to include demolition explosives (for example, detonation cord, C-4 blocks of explosives, and so on).
 - (5) One or more semiautomatic or manually operated firearms.
 - (6) Five or more rounds of ammunition greater than .50 caliber.
 - (7) 1,000 or more rounds of .50 caliber or smaller ammunition.
- i.* Actual or attempted break-ins of arms rooms or storage areas for AA&E.
- j.* Armed robbery or attempted armed robbery of AA&E.
- k.* Any evidence of trafficking of AA&E, such as bartering for narcotics or any other thing of value, to include taking AA&E across international borders, regardless of the quantity of AA&E involved.
- l.* Aggravated arson.
- m.* Except for deaths occurring due to natural causes (such as pre-existing illness, disease or medical condition, to include hospice care) in medical treatment facilities, all deaths occurring on Army installations must be reported, including but not limited to, accidents, homicides, suicides, highly communicable and lethal diseases, or other incidents. All deaths of Soldiers, regardless of duty status, that occur off the installation will be reported. Additionally, deaths of Family members that occur off the installation, which are deemed to be criminal in nature, will be reported. If the manner of death of Soldier or Family member is unknown, the incident will be reported as “undetermined manner of death” and the manner of death will be updated by add-on SIR as soon as determined. Next-of-kin notification, use of seatbelt and PPE, and alcohol or drug use will be included in the initial SIR or updated accordingly in the add-on SIR.
- n.* Kidnapping.
- o.* Major fires or natural disasters involving death, serious injury, property damage in excess of \$250,000, or damage that seriously degrades unit operational or training capabilities.
- p.* Group breaches of discipline involving 10 or more persons who collectively act to defy authority.
- q.* Training and troop movement accidents resulting in serious injury or death.
- r.* Maltreatment of Soldiers or DA civilians to include assaults, abuse, or exploitation where the offender has a trainer, supervisor, or cadre-trainee relationship with the victim, regardless of whether they are members of the same organization. Instances of consensual sex are not reportable, unless other considerations such as sexual harassment or adverse publicity are involved.
- s.* Violations of Army policy as it pertains to monitoring and recording of conversations in accordance with AR 190-30 and AR 190-53, or acquisition and storage of non-affiliated U.S. person information in accordance with AR 380-13.
- t.* Actual or alleged incident of child abuse that takes place within an Army organizational setting or facility (for example, child development center, youth activities center, MTF, gymnasium, and so forth). Actual or alleged incident of child abuse that takes place within an Army-sponsored or -sanctioned activity (for example, quarters-based Family childcare home, youth sports or recreation activities, field trips, and so forth). This paragraph also applies to incidents of child abuse occurring within the family unit which involve the use of a weapon (for example, a firearm, knife, or other devices which will cause serious bodily injury), the victim suffers a broken limb, is sexually abused, is choked or strangled, or is admitted to the hospital because of injuries incurred during the incident.
- u.* Serious child injury or death, not resulting from child abuse, while the child is in the Army’s care at a nonmedical facility (child development center, quarters-based Family childcare home, youth activities center, and so

forth) or within an Army-sponsored or -sanctioned activity. This paragraph does not apply to sports injuries related to, or potentially inherent in, a youth activity or event.

v. Serious domestic violence incidents (unrestricted reporting only). This report will include whether the Soldier listed as a subject was deployed within the past year leading up to the incident.

w. Incidents involving firearms that cause injury or death.

x. Federal crimes reportable under AR 381-10, when they meet reporting criteria.

y. Any other incident that the commander determines to be of concern to HQDA based on the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

8-4. Category 3 reporting criteria

IMCOM regional directors, and ACOM, ASCC, and DRU commanders (excluding USACIDC) will, by approved supplementation to this regulation, establish additional reporting criteria to be known as “category 3.” Means and format for reporting will be as prescribed by the IMCOM regions, ACOM, ASCC, and DRU commanders, with the requirement that numbering sequences for category 3 reports will be separate from those used for reports to HQDA.

8-5. Operational reporting reports

a. Commanders will use the operational reporting-3 (OPREP-3) format when reporting incidents meeting Chairman of the Joint Chiefs of Staff (CJCS) reporting criteria, outlined in CJCSM 3150.03D.

b. Commanders are responsible for timely and accurate reporting of all events or incidents meeting CJCS reporting criteria, as outlined in CJCSM 3150.03D. The requirements of this paragraph are for OPREP-3 pinnacle (OPREP-3P) reports and will follow the guidance of CJCSM 3150.03D, Enclosure A, Appendix A. The following criteria may also be considered for incidents potentially requiring one of the other OPREP-3 reports (non-pinnacle):

(1) Generates a higher level of military action.

(2) Causes a national reaction.

(3) Affects international relations.

(4) Causes immediate widespread coverage in news media.

(5) Is clearly against national interest.

(6) Affects current national policy.

c. If in doubt whether an incident meets the above-listed criteria, submit an OPREP-3 report, and the receiving agency will make the determination on further actions to take.

d. Should an incident be both OPREP-3 and SIR reportable, the OPREP-3 report will include basic information, ensuring it does not divulge information that may hinder an ongoing investigation. The SIR contains detailed information and will be protected from widespread or improper release and classified as a “law enforcement sensitive/ FOUO” report.

e. Commanders submit OPREP-3 reports through their own chain of command to HQDA Army Operations Center per the existing reporting requirements. If the chain of command does not include an ASCC, the senior commander will simultaneously submit the OPREP-3 to their chain of command, HQDA, and the ASCC assigned responsibility for the geographic combatant command. Each ASCC is responsible for forwarding the OPREP-3 to their respective geographical combatant commander and to the HQDA Army Operations Center for the SA.

8-6. Incidents reportable by means other than serious-incident reports

The events or incidents listed below may be reported by means other than SIRs.

a. Those operational events reported according to Joint Chiefs of Staff Publication 6-0.

b. Aircraft accidents and related mishaps, unless they meet other SIR criteria.

c. Nuclear weapons accidents or incidents.

d. Nuclear reactor mishaps.

e. Incidents involving foreign students.

f. Requests from civil authorities for military support of civil disturbances or counter-terrorist operations.

g. Incidents involving national security crimes and deliberate security compromises will be reported to the nearest Army CI office as required by AR 381-12.

h. Incidents covered under Executive Order 12333, as implemented by DOD 5240.1-R.I.

8-7. Suspicious activity report

The Army will use eGuardian to report, share and analyze unclassified suspicious activity information regarding potential threats or suspicious activities affecting DOD personnel, facilities, or forces in transit in both CONUS and OCONUS. USACIDC is the Army’s eGuardian program manager.

a. eGuardian is the Federal Bureau of Investigation’s (FBI) sensitive-but-unclassified web-based platform for reporting, and in some instances, sharing, suspicious activity and threat related information with other federal, state, tribal, and territorial law enforcement and force protection entities. Information entered into eGuardian by the Army

may be either shared with all eGuardian participants or reported directly to the FBI. All information entered into eGuardian by the Army will comply with the policy framework for the system and any existing agency agreements, which incorporate privacy protections. Analysis of SARs will assist CRIMINTEL analysts and commanders in mitigating potential threats and vulnerabilities, and developing annual threat assessments.

b. eGuardian user, supervisor, approver, or read-only access is limited to LE personnel and LE CRIMINTEL analysts, to include those assigned to the U.S. Army counterintelligence law enforcement cell and the HQDA antiterrorism operations and intelligence cell. The following definitions apply for eGuardian access:

(1) LE personnel and LE CRIMINTEL analysts are assigned, attached or detailed to LE activities, validated (in writing) to support LE missions.

(2) DOD contractors who, on behalf of the Army are involved in the SAR process, to include operating a system of records, and any of the activities associated with maintaining a system of record, such as collecting and disseminating records.

(3) Army entities with LE missions, including force protection, will be provided access.

(4) Antiterrorism and force protection officers, employed in support of Army LE agencies.

c. Access does not apply to the following categories of Army personnel, who are not considered to be Army LEOs:

(1) Security officers not employed as an Army LE analyst or criminal intelligence analyst and not validated, in writing, by the Army.

(2) Antiterrorism and force protection officers not validated in law enforcement or law-enforcement-supporting positions.

(3) Counterintelligence officers or counterintelligence special agents.

(4) Corrections specialists who are not Army LEOs.

d. Agencies with intelligence and CI missions are restricted from acquiring eGuardian accounts. However, LE personnel will provide eGuardian SAR information to CI and intelligence analytic cells upon indications of attempted or actual espionage, subversion sabotage, terrorism-extremist activities directed against the Army and its personnel, facilities, resources, and activities; indicators of potential terrorist-associated insider threats; illegal diversion of military technology; unauthorized intrusions into automated information systems; unauthorized disclosure of classified information; and indicators of other incidents that may indicate foreign intelligence or international terrorism targeting of the Army. This is to ensure appropriate SAR data is fused with other intelligence reporting.

e. Any concerned Soldier or citizen can submit an SAR to the nearest installation PM, DES, CI, or CID office. The receiving office will then be responsible for reviewing the information and determining whether it is appropriate for submission into eGuardian.

f. This reporting does not negate the requirement to dispatch serious-incident reports through Army and LE reporting channels. Army activities without an installation PM or DES will refer to table 1-1 to find their supporting installation PM or DES.

g. Each installation PM or DES will do the following:

(1) Conduct a preliminary evaluation of SAR information received to assess credibility, and initiate an RDF, only when the incident warrants immediate investigation or when the SAR is recommended as an eGuardian report. The report will be coordinated with the supporting CID office and receive supervisory-level approval, prior to entering into eGuardian. Any installation PM or DES without user access will forward SARs using the RDF, to the local CID office, for entering into eGuardian. An urgent-classification SAR will be entered as a restricted entry in the MP blotter to preclude compromise of the information. The PM or DES will ensure use of offense codes under the 9Z category, along with the RDF or blotter entry number, to identify the information as SAR.

(2) Ensure that sufficient installation PMO or DES personnel have eGuardian access (user, supervisor, read-only) in order to establish situational awareness of SAR information entered into the eGuardian system.

(3) Ensure CI-applicable SAR information is reported to the local CI activity in accordance with AR 381-12, and affected commanders for the purposes of supporting antiterrorism decisions, in accordance with AR 525-13.

(4) Coordinate CID assistance in conducting preliminary and follow-on SAR investigations.

h. eGuardian reportable and nonreportable information is defined according to many variables:

(1) Reportable information categories—

(a) Urgent: refers to information regarding a terrorism-related event, terrorist threat, or suspicious activity. Urgent information will be submitted into eGuardian for approval in not more than 12 hours of receipt. For example, if a stolen vehicle is recovered on a DOD installation and contains firearms and a laptop computer with information pertaining to planned attacks on a government facility.

(b) Specific and actionable: those reports warranting the initiation of investigative activity. These reports will be submitted into eGuardian for approval within 24 hours. For example, if security guards observe a person taking prolonged video of the entrance to a DOD facility with a handheld video recorder, and the same individual is reported to have been observed recording video of the building on two separate occasions in the past week.

(c) Non-actionable: those reports that may be relevant to the establishment of patterns of suspicious activity. These

reports will be submitted into eGuardian for approval within 72 hours. (For example: military uniforms are reported stolen out of an employee's vehicle while parked at Baltimore Washington International Airport.)

(2) In accordance with DTM 10-018, the following are examples of nonreportable or inappropriate information:

(a) Information based solely on the ethnicity, race, or religion of an individual, or reported solely due to the exercise of rights guaranteed by the first amendment (for example, authorized protests).

(b) Information gathered under 50 USC 1801, et seq. (The Foreign Intelligence Surveillance Act).

(c) Information classified confidential, secret, top secret, or compartmented. This information is reported using the classified guardian system. USACIDC elements needing to report this type of information will forward it to the Headquarters CIOC, or report the information via intelligence information reports. CIOC analysts will ensure the USACIDC liaison officer to the National Joint Terrorism Task Force receives the information for submission as a guardian report.

(d) Information pertaining to Rule 6(e) (grand jury materials) of the Federal Rules of Criminal Procedure.

(e) Any information otherwise legally restricted.

Chapter 9

Reporting Procedures for Serious-Incident Reports

9-1. Special handling of reports

Reports submitted according to this regulation are LE reports in accordance with AR 25-55. They will be assigned a proper security classification according to AR 380-5 or marked with a minimum classification of FOUO according to AR 25-55. Reports or any information from them will be released according to AR 25-55 and this regulation.

a. The stipulations of 5 USC 552a (The Privacy Act of 1974) apply to SIRs in accordance with AR 340-21. Dissemination and use of SIRs will be restricted to persons who need the reports to perform their official duties.

b. All SIRs will include the following or similarly worded statement: "In accordance with AR 340-21, AR 190-45, and DOD 5400.7-R, information contained in this report is law-enforcement sensitive, confidential and private in nature, and any further distribution (forwarding to unauthorized personnel) without the authorization of the (insert reporting command's installation PM or DES) will be in violation of the UCMJ and USC."

9-2. Time requirements and means of reporting

a. *Category 1 serious incident.* Category 1 serious incidents will be reported by telephone to the Army Watch immediately upon discovery or installation level notification (within 4 hours). The telephonic report will be in the format in figure 9-1. It will be followed by a written report, preferably by electronic mail or if electronic mail is not available, by electronic message, to the Army Watch within 12 hours of discovery or notification. Facsimile will be used as a supplemental transmission.

b. *Category 2 serious incidents.* Category 2 serious incidents will be reported by electronic mail or if electronic mail is not available, by electronic message to the Army Watch within 24 hours of discovery or notification at the installation level. Facsimile will be used to supplement the transmission. (See app C for electronic mail addresses, electronic message addresses, and facsimile numbers.)



DEPARTMENT OF THE ARMY

ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

ABCD-EF

(date)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Law Enforcement Report – SIR (Category 2) /Initial/Final– 12345-2014-MPC999-012345-7F8B2

1. Offense: Missing/Stolen Ammunition (Founded).
2. Date/Time/Location of Occurrence: 0700, 1 Apr 14 – 1630, 1 Apr 14, Range 1, Fort Swampy, XY.
3. Date/Time Reported: 1700, 1 Apr 14.
4. Investigated By: SGT John Doe.
5. Subject/Suspect: Unknown; Missing Ammunition (Founded).
6. Victim: US Government (A Co. 1/1st Mess Kit Bn, 1 BCT, 999th Sustainment Div, Fort Swampy, XY); Missing Ammunition (Founded).
7. Report Summary: Information in this report is based upon an allegation or preliminary investigation and may change prior to completion of the report.

CPT [Name], A Co. 1/1st Mess Kit Bn, reported that his unit had picked up a million rounds of 5.56mm ammunition for training on the morning of 1 Apr 14, and that as they were closing down the range, it was discovered that 50 rounds of 5.56mm were unaccounted for. Searches of the area, all vehicles and all personnel failed to recover the missing ammunition. Value of the missing ammunition is \$10.15. This is terminal report. No further law enforcement action is anticipated.

8. Unique Circumstances:
Subject Position:
Victim Position:
Relationship:

Figure 9–1. Format and instructions for preparing a serious incident report

ABCD-EF
SUBJECT: Law Enforcement Report – SIR (Category 2)/Initial/Final– 12345-2014-
MPC999-012345-7F8B2

9. Media Interest: None.

10. Additional Information: None.

11. Exhibits: None.

Commanders are reminded of the provision of AR 600-8-2 pertaining to suspension of favorable personnel actions (flagging) and AR 380-67 for the suspension of security clearances of persons under investigation. Army law enforcement reports are exempt from automatic termination of protective marking IAW Chapter 3, AR 25-55. IAW AR 340-21, AR 190-45 and DODI 5400.7-R, information contained in this report is law enforcement sensitive, confidential and private in nature, and any further distribution (forwarding to unauthorized personnel) without the authorization of the Provost Marshal General will be in violation of the UCMJ and USC.

Report Prepared By

Report Approved By:

SGT Doe

1LT [Name]

Signature Authority

PM [First, Last Name]

DISTRIBUTION
Cdr, Ft Swampy
C/S, Ft Swampy
PM, Ft Swampy
SJA, Ft Swampy
etc

Figure 9–1. Format and instructions for preparing a serious incident report, continued

9–3. Types of serious-incident reports and reporting formats

There are three types of SIRs—

a. The SIR, which is the original submission. Figure 9–1, above, shows an example of the most commonly used type of SIR, the SIR initial/final report.

b. The SIR supplemental submitted to provide information not available at the time of the original report or when more pertinent information, such as results of autopsy, identification of subject, recovered AA&E or sensitive items, and so on is developed, or in response to a request for more information from HQDA.



DEPARTMENT OF THE ARMY

ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

ABCD-EF

(date)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Law Enforcement Report – SIR (Category 2)/Final Supplemental – 12345-2014-MPC999-012345-7F8B2

1. Offense: Missing/Stolen Ammunition (Unfounded).
2. Date/Time/Location of Occurrence: 0700, 1 Apr 14 – 1630, 1 Apr 14, Range 1, Fort Swampy, XY.
3. Date/Time Reported: 1700, 1 Apr 14.
4. Investigated By: SGT John Doe.
5. Subject/Suspect: Unknown; Missing Ammunition (Unfounded).
6. Victim: US Government (A Co, 1/1st Mess Kit Bn, 1 BCT, 999th Sustainment Div, Fort Swampy, XY); Missing Ammunition (Unfounded).
7. Report Summary:

CPT [Last Name], A Co. 1/1st Mess Kit Bn, reported that his unit had picked up a million rounds of 5.56mm ammunition for training on the morning of 1 Apr 14, and that as they were closing down the range, it was discovered that 50 rounds of 5.56mm were unaccounted for. Searches of the area, all vehicles and all personnel failed to recover the missing ammunition. Value of the missing ammunition is \$10.15. This is terminal report. No further law enforcement action is anticipated.

On 15 Apr 14, Mr. [First, Last Name], Supervisor, Ammunition Supply Point (ASP), reported that the missing box of 50 rounds of 5.56mm ammunition had been found in an ASP bunker. It had apparently been left behind when the unit picked up its ammunition draw.

Figure 9–2. Format for a serious incident report add-on, which is used to update an earlier report

ABCD-EF
SUBJECT: Law Enforcement Report – SIR (Category 2)/Final Supplemental – 12345-2014-MPC999-012345-7F8B2

8. Unique Circumstances:

Subject Position:
Victim Position:
Relationship:

9. Media Interest: None.

10. Additional Information:

None

11. Exhibits: None.

Commanders are reminded of the provision of AR 600-8-2 pertaining to suspension of favorable personnel actions (flagging) and AR 380-67 for the suspension of security clearances of persons under investigation. Army law enforcement reports are exempt from automatic termination of protective marking IAW Chapter 3, AR 25-55. IAW AR 340-21, AR 190-45 and DODI 5400.7-R, information contained in this report is law enforcement sensitive, confidential and private in nature, and any further distribution (forwarding to unauthorized personnel) without the authorization of the Provost Marshal General will be in violation of the UCMJ and USC.

Report Prepared By

Report Approved By:

SGT Doe

1LT [Last Name]

Signature Authority

PM [First, Last Name]

DISTRIBUTION
Cdr, Ft Swampy
C/S, Ft Swampy
PM, Ft Swampy
SJA, Ft Swampy
etc

Figure 9–2. Format for a serious incident report add-on, which is used to update an earlier report, continued

9-4. Protected identity

Every effort will be made to protect the identity of those individuals listed as a PI in the report that served as the basis for generating a SIR (this includes the subject if he or she was listed as a PI in the initial report). No information will be included in the SIR that will reveal the identity of the PI; for example, the name, address, unit, or duty position.

9-5. Reporting incidents when reporting responsibility is transferred

When reporting responsibility is transferred between commands—

a. The first report submitted after an agreed transfer will contain the name and SIR number of the original submission and a statement added to the “Remarks” paragraph that reporting responsibility was transferred.

b. The command and IMCOM region accepting SIR transfer will provide the relinquishing command an information copy of all future reports on the incident.

9-6. Required information addressees on serious-incident reports

Commanders will ensure that information addressees are included on SIRs as follows:

a. For all SIRs, the reporting command’s ACOM, ASCC, or DRU, the respective IMCOM region, and the USACIDC, to include local CID offices.

b. If the incident involves personnel or equipment of another unit, then the installation, IMCOM region, ACOM, ASCC, or DRU installation or facility; that unit, installation, or facility and its respective higher headquarters will be information addressees.

c. If the incident involves ARNG personnel, facilities, or equipment, the respective State government’s Adjutant General and the National Guard Bureau will be information addressees.

d. If the incident involves USAR personnel, facilities, or equipment, the Commander, U.S. Army Reserve Command (USARC), will be an information addressee.

e. If the incident involves MP personnel as the subject of a criminal offense or other misconduct, the Commandant, U.S. Army Military Police School will be an information addressee.

f. If the incident involves threats to the President of the United States, other high-ranking Government officials, or anyone under the protection of the USSS, then the USSS and the Defense Intelligence Agency will be information addressees.

g. If the incident involves nonappropriated fund personnel, resources, or property, child abuse, or the injury or death of a child in an Army organizational setting or Army-sponsored activity (see paras 8-3*t* and 8-3*u*), or serious domestic violence (see para 8-3*v*), the Commander, U.S. Army Community and Family Support Center, will be an information addressee.

h. If the incident involves Federal crimes reportable under AR 381-10 and this regulation, include the Army General Counsel as a “To” addressee and HQDA Deputy Chief of Staff, G-2 (DAMI-CD) as an information addressee.

Chapter 10

U.S. Magistrate Court

10-1. Relationship to Army

The U.S. Magistrate Court provides the DA with the means to process and dispose of certain categories of misdemeanors by mail or through appearance in magistrate court. The U.S. Magistrate Courts and U.S. District Courts will, by local court rules, establish the payment of a fixed sum in lieu of court appearance in cases involving certain misdemeanors.

10-2. U.S. Magistrate Court objectives

The U.S. Magistrate Court provides the following:

a. Uniform procedures for the collection of fines, the forfeiture of collateral in lieu of fines, the forfeiture of collateral in lieu of appearance, the scheduling of mandatory hearings or voluntary hearings requested by defendants, and the keeping of records.

b. A method of accounting for fines, for collateral, and for Central Violations Bureau Forms issued.

c. Convenience to the public.

d. Enforcement of misdemeanors, or violation of laws on Army installations.

10-3. Court appearances

a. Each court will determine, by local court rule, which offenses require mandatory appearances by violators.

Installation PMs, DESs, or other LE officials will coordinate through installation SJAs, with local U.S. magistrates, or U.S. District Courts to secure a court-approved list of offenses requiring mandatory appearance before the local U.S. magistrate.

b. Optional appearances will be requested by violators:

(1) *At the time a Central Violations Bureau Form is issued.* The LE officials issuing the Central Violations Bureau Form will refer violators to the proper U.S. magistrate if a hearing is requested by the violator.

(2) *By mail.* These violators include those who—

(a) Are not present at the time a Central Violations Bureau Form is issued (for example, for a parking violation).

(b) Subsequently volunteer to appear before the U.S. magistrate rather than forfeit the collateral indicated on the Central Violations Bureau Form.

(c) Violators who use the mail-in procedure to request an optional appearance before a U.S. Magistrate must place a check mark on the appropriate line. The violator will be notified by the clerk of the U.S. District Court of the time, date, and place to appear for the hearing.

10–4. Central Violations Bureau

a. The Administrative Office of the U.S. Courts established the CVB for processing Central Violations Bureau Forms. Each U.S. District Court has a local rule or order that provides or authorizes a preset forfeiture of collateral amount for persons charged with certain petty offenses. Rules for processing misdemeanors and other petty offenses are established under Rule 58 of the Federal Rules of Criminal Procedure and by the individual district courts. The existence of the local rules does not prevent LE personnel from requesting that a complaint be filed against a defendant in lieu of issuing a Central Violations Bureau Form. These procedures merely provide an alternative method for handling petty offense cases; a method which is usually more convenient for the law enforcement personnel, the defendant, and the court.

b. Even though the amount paid is stated to be a fine, it is actually a posting of collateral which is forfeited if the defendant pays and does not request an appearance before a U.S. magistrate judge. Acceptance of payment by the CVB terminates the proceeding. Local Federal rules and State law determine whether a moving violation will be reported as a conviction to the state Department of Motor Vehicles (DMV). There are certain offenses where forfeiture of collateral is not permitted. Those offenses require a mandatory appearance before a U.S. magistrate judge. Also, a defendant will request a hearing before a U.S. magistrate judge rather than paying the forfeiture of collateral and a hearing will be scheduled. The CVB or the U.S. magistrate judge will process these matters.

c. The U.S. Attorney is responsible for all prosecutions in the U.S. District Court and for coordinating law enforcement efforts. Generally, the U.S. Attorney delegates to the individual agencies authority to issue Central Violations Bureau Forms and to prosecute petty offenses initiated by Central Violations Bureau Form. As an example, judge advocates have generally been authorized by the U.S. Attorney to prosecute certain crimes in which the Army has an interest. These are commonly referred to as Special Assistant United States Attorneys.

Chapter 11

Use of United States District Court Central Violations Bureau Form

11–1. General

a. The basis for initiating action by the U.S. magistrate system is the United States District Court Central Violations Bureau Form. The form is designed to provide legal notice of a violation. It also records information required by the U.S. District Court, LE authorities, and, if appropriate, state DMVs. The three-part form is printed on chemically carbonized paper and pre-numbered in a series for accounting control. The form will be bound with 25 Central Violations Bureau Forms per book. Installation LE agencies will be accountable for each Central Violations Bureau Form issued and for stock on-hand. Accountable records will be maintained in accordance with AR 25–400–2.

b. The installation PM or DES, or other LE officials, will coordinate through installation SJAs with the U.S. magistrate of the judicial district in which the installation is located. As a minimum, information listed below must be obtained from the U.S. magistrate before referral of violators to the U.S. magistrate or U.S. District Court.

(1) A list of misdemeanors for which the mail-in procedure is authorized and the amount of collateral for each offense. The district court address will be pre-stamped (using a locally procured stamp) on the violator's copy of the Central Violations Bureau Form by the issuing authority.

(2) A list of misdemeanors requiring mandatory appearance by the violator before the U.S. magistrate. The magistrate's name and location, and the dates and times of appearance, will be cited when scheduling a violator to appear before the U.S. magistrate.

c. The Statement of Probable Cause and the Promise to Appear will be used in compliance with installation SJA and U.S. magistrate or U.S. District Court policies and instructions. The Statement of Probable Cause printed on the back of the original United States District Court Central Violations Bureau Form is required to support the issuance of a

summons or an arrest warrant. The promise to appear, printed with instructions to the violator on the inner flap of the envelope, is optional and some U.S. magistrates or U.S. District Courts will elect not to use it.

11-2. Important guidelines for issuing the U.S. District Court Central Violations Bureau Form

The following is a list of important guidelines for the preparation of the U.S. District Court Central Violations Bureau Form:

- a.* Complete the Central Violations Bureau Form legibly. Printing is preferred.
- b.* Ensure the CVB location code is on every Central Violations Bureau Form.
- c.* Mail Central Violations Bureau Forms to the CVB within 5 days of being issued to the defendant.
- d.* Only one offense will be cited per Central Violations Bureau Form.
- e.* Ensure the proper forfeiture schedule is used for the appropriate U.S. District Court.
- f.* Do not indicate the fine amount on mandatory appearance violations.
- g.* Verify that the lockbox address (Central Violations Bureau, P.O. Box 70939, Charlotte, NC 28272-0939) appears on the defendant's copy to ensure proper mailing.

11-3. Issue and disposition procedures

- a.* Information entered on the U.S. District court Central Violations Bureau Form is dependent on the following:
 - (1) The type of violation (standing, moving traffic violation, or nontraffic offense).
 - (2) Whether the violation cited requires the mandatory appearance of the violator before a U.S. magistrate.
- b.* A standardized Central Violations Bureau Form initiates a petty offense case in a U.S. District Court. It is a multipart document designed to provide legal notice to the defendant and to provide the court and the agency with necessary information for processing.
- c.* Each Federal LE agency is responsible for providing its personnel with Central Violations Bureau Forms. Each agency is also responsible for accounting for all Central Violations Bureau Forms.
- d.* The Central Violations Bureau Form is a three-part form which is distributed as follows:
 - (1) The white (original) copy is mailed to: Central Violations Bureau, P.O. Box 780549, San Antonio, TX 78278-0549.
 - (2) The pink copy is kept by the issuing agency. The CVB recommends 5 years in accordance with records retention guidelines.
 - (3) The ivory (cardboard) copy is given to the defendant at the time of issuance; or upon arrest, it is placed on the defendant's vehicle or mailed to the defendant by the issuing agency. This copy should contain the address of the lockbox facility on the front of the envelope. This copy informs the defendant of the charges and gives detailed instructions on how to pay the collateral or plead not guilty and appear in court. The instructions also advise the defendant of the potential consequences for failure to appear or to pay, including notifying the state DMV, which could affect their driving privileges and/or registration. The citation also serves as an envelope for mailing forfeiture of collateral payment to the lockbox facility. The issuing officer must complete certain items on the Central Violations Bureau Form in order to provide the CVB with all necessary information for the U.S. magistrate judge.

11-4. Fines, collateral, and nonpayment delinquencies

Army LE agencies will do the following:

- a.* Not accept or otherwise collect any fines or collateral or keep records of fines or collateral paid or not paid.
- b.* Take no action concerning nonpayment delinquencies except where warrants are issued for the violator by the proper court authorities.

11-5. Notification to commanders and supervisors

When the Central Violations Bureau Form is used to cite military personnel and DOD-affiliated employees for misdemeanors, the violator's unit commander or supervisor will be advised as follows:

- a.* When the Central Violations Bureau Form is used to cite military personnel and DOD-affiliated employees for mandatory appearance type violations, an information copy of the LER will be provided to the violator's unit commander or supervisor. The LER will denote the date, time, location, type of violation, and where the violator is scheduled to appear before the U.S. magistrate. The LER will be entered in DA Form 190-45-SG, also known as ALERTS. DA Form 4833 will be generated and used to report action taken by the commander or supervisor.
- b.* When the Central Violations Bureau Form is used to cite military personnel and DOD-affiliated employees for violations that are disposed of by mail, the commander or supervisor will be advised by use of the LER. The LER will be entered into the automated DA Form 190-45-SG, also known as ALERTS. DA Form 4833 will be generated and used to report action taken by the Magistrate Court to the commander or supervisor. The installation PM, DES, or other designated person will sign DA Form 4833 before forwarding it to the commander.

11-6. Use of statement of probable cause

In compliance with guidelines issued by the Administrative Office of the U.S. Courts, the reverse side of the Central

Violations Bureau Form provides the statement of probable cause. This is required by Rule 58(d)(3) of the Federal Rules of Criminal Procedure to support the issuance of a summons or arrest warrant. The statement of probable cause will be printed on the reverse side of the original Central Violations Bureau Form, on all copies of the Central Violations Bureau Form, or as a separate form (such as DA Form 2823). Upon receipt of the probable cause statement by the issuing officer and a finding of sufficient probable cause by the U.S. magistrate judge, bench warrants forwarded by the CVB to the U.S. magistrate judge will then be signed, dated, and issued. If the statement of probable cause has been properly completed by LE personnel, the U.S. magistrate judge can then issue the bench warrant.

11-7. Mandatory appearance

Certain offenses require a mandatory appearance before a U.S. magistrate judge. When preparing such a Central Violations Bureau Form, LE personnel will check the box indicating mandatory appearance. The place and time box of the court appearance will not be completed, unless the CVB or the court authorizes the court date and times to be written on the Central Violations Bureau Form. The CVB will notify the defendant of this information by mailing to the defendant a notice to appear (NTA) letter. The CVB will either promptly forward the Central Violations Bureau Form to the designated U.S. magistrate judge to schedule, or CVB will schedule the court appearance. If LE personnel check the box indicating mandatory appearance, then the box indicating a collateral fine will be left blank.

11-8. Submitting mandatory hearing violations

In most districts, mandatory appearance Central Violations Bureau Forms are transmitted to U.S. District Court in the same manner as optional appearances. Other districts require mandatory appearance violations be mailed directly to the U.S. magistrate judge's office. If the hearing date and time has not been preassigned, it is the responsibility of the U.S. magistrate judge's staff to notify the defendant and the agency of the date.

11-9. Submitting forms to the Central Violations Bureau

Agencies should submit Central Violations Bureau Forms within 5 days, in person or by mail. Central Violations Bureau Forms should be forwarded to the CVB the same day the Central Violations Bureau Forms are issued. Transmittal sheets are not required by CVB, but can be used if the agency so desires. If an agency requires a receipt for the notices, they will include the transmittal sheet and a self-addressed, pre-stamped envelope. The transmittal sheet will be stamped "received," and returned to the agency. This merely acknowledges receipt of the Central Violations Bureau Forms.

11-10. Agency requests to dismiss or void a Central Violations Bureau form

a. If a Central Violations Bureau Form has been issued in error, it will be voided in one of two ways. If the agency is still in possession of all copies, void the notice and record that action. If the Central Violations Bureau Form has already been placed on a vehicle, given to the defendant, or has been forwarded to the CVB, the notice can only be dismissed by the U.S. magistrate judge for that district.

b. A written statement signed by the supervisor or chief LE officer from an agency requesting a Central Violations Bureau Form or notices be dismissed or voided must be forwarded to the CVB via mail or emailed to the following address: cvb@cvb.uscourts.gov. The mailing address is: Central Violations Bureau, P.O. Box 780549, San Antonio, TX 78278-0549. The CVB will enter a request for void into the database and forward it to the U.S. magistrate judge with a CVB transmittal letter. Upon reviewing the request from the agency, the U.S. magistrate judge will either approve or deny dismissal.

(1) To approve the dismissal or void, the U.S. magistrate judge will check the block "Dismissal Approved," date, sign, and forward the order to the CVB. The CVB will enter the disposition code NA (Agency Requested Dismissal) into the system and file all related paperwork.

(2) To deny the dismissal or void, the U.S. magistrate judge will check the block "Further Action to Be Taken," date, sign, and forward the order to the CVB. The CVB will then contact the agency and inform them of any additional information or action ordered by the U.S. magistrate judge.

c. If an RDF was initiated, the report should be updated in the automated DA Form 190-45-SG, also known as ALERTS, to reflect that the Central Violations Bureau Form was dismissed or voided.

11-11. Request for dismissal or void by the defendant

When a defendant mails evidence to the CVB concerning the offense, (proof of insurance, registration, and so on), or correspondence addressed to the U.S. magistrate judge directly, the information is entered into the computer and forwarded to the U.S. magistrate judge attached with the docket package. In some instances, a citation or citations will have already been forwarded to the court. These cases will be attached to a CVB transmittal letter and forwarded to the U.S. magistrate judge.

a. To approve the dismissal or void, the U.S. magistrate judge will check the block "Dismissal Approved," will date, sign, and forward the order to the CVB. The CVB will enter the disposition code "NH" (violation request) into the system and file all related paperwork.

b. To deny the dismissal or void, the U.S. magistrate judge will check the block "Further Action to Be Taken," date,

sign, and forward the order to the CVB. The CVB will then contact the agency and inform them of any additional information or action ordered by the U.S. magistrate judge.

11–12. Central Violations Bureau Forms issued to unattended vehicles

Central Violations Bureau Forms may be issued to unattended motor vehicles. If at all possible, the issuing agency must ascertain the defendant's name and address before the Central Violations Bureau Form is forwarded to CVB. Central Violations Bureau Forms without a complete mailing address will be returned to the agency for further action.

11–13. U.S. magistrate judge docket report

The NTA letters are mailed to defendants approximately 4 weeks before the court date to allow for a response from the defendant and to allow the defendant to forfeit collateral. If the CVB does not hear from the defendant, a computer generated docket sheet and judgment order is automatically produced 14 days before the court date. Warrants, suspensions, and images of the original Central Violations Bureau Form are then forwarded to the U.S. magistrate judge with the docket sheet and judgment order, which lists the violation number, CVB location code, and the defendant's name and address. The violations are listed in alphabetical order according to the defendant's last name. The docket sheet and judgment order has additional space for the U.S. magistrate judge's courtroom deputy to complete at the time of the hearing. Once the hearing is held, the information will be entered on the docket sheet and judgment order and returned to CVB.

11–14. Request to agency for a better address

The CVB requests agencies mail all original citations within 3 working days of issuance. Central Violations Bureau Forms without full name and address information should not be mailed, unless payment has been received by CVB. Central Violations Bureau Forms received at the CVB without a complete mailing address will be returned to the agency for further action. If a Central Violations Bureau Form is entered without a valid address or returned to the CVB as undeliverable, a request for a better address will be generated. If the agency obtains a better address for these violations, please notify CVB. Failure to receive better addresses from the issuing agency within 15 days from the date of this list will result in the voidance or dismissal of these violations.

11–15. Undeliverable warning letters referred to U.S. magistrate judge

Sixteen days after the transmittal "Request to Agency for Better Address" has been printed and forwarded to the agency, and no response has been received, an "Undeliverable Warning Letters Referred to U.S. Magistrate Judge" transmittal will be produced by the CVB. This transmittal will have images of the original Central Violations Bureau Forms attached and will be forwarded to the U.S. magistrate judge. The U.S. magistrate judge has the following two options:

a. To approve dismissal for lack of a better address, the U.S. magistrate judge will check the block "Dismissal Approved," date, sign, and return the transmittal to the CVB. The CVB will enter the disposition code "NM" (dismissal without prejudice) into the system and file all related paperwork. Agencies will be notified of the disposition by issuance of the "open/closed index" monthly report.

b. To deny dismissal for lack of a better address, the U.S. magistrate judge will check the block "Further Action to be Taken," and then date, sign, and return the transmittal to the CVB with instructions on any action to be taken by the CVB or issuing agency.

11–16. Notice to appear letters

a. The NTA letters are mailed to defendants 4 weeks prior to the court date. The NTA letter lists the citation number, location code, date of offense, amount that will be forfeited in lieu of going to court (if the offense committed requires a mandatory appearance, the NTA will read "mandatory appearance required"), the date the NTA letter was mailed, the offense, place of offense, and any special instructions the court wishes the defendant to know. The NTA letter will notify the defendant of the location, date and time of hearing. Each NTA letter contains a postage paid business reply envelope. In the event the offense was an "optional appearance," the defendant has the opportunity of paying the citation prior to the court date.

b. Defendants have the option of calling to obtain their court date from the automated voice case information system at the CVB. A selection on the automated answering system allows them to enter their violation number, and after doing so, the recording will repeat the court date and time. Should the defendants have any questions, an operator will assist them.

11–17. Warrant

The warrant reflects the defendant's name and address, the violation number, the date the Central Violations Bureau Form was issued, and the offense. If the court date has passed and the defendant has failed to appear, the U.S. magistrate judge may issue a warrant. The "notice before arrest" is mailed by the U.S. Marshal to the defendant, upon receipt of the warrant from the U.S. magistrate judge.

11–18. Suspension notices

If legislation in a state allows acceptance of a Federal citation from the CVB by the state DMV, a defendant who does not pay the forfeiture of collateral amount and does not appear before the U.S. magistrate judge on the scheduled court date may have their State-issued driver's license suspended. The CVB will produce a suspension notice to mail to the court together with the final docket. The suspension process normally takes the place of the warrant process. If the court decides to issue the suspension, then the court is responsible for mailing a copy to the defendant and to the DMV, and for retaining a copy for the court's records. If the defendant pays the forfeiture of collateral amount after receiving notice of the suspension, the court should submit a withdrawal of the suspension to the State government's DMV.

11–19. Agency notification

When the U.S. magistrate judge docket is produced by the CVB, a report (the "magistrate-referred listing") of violations is emailed to all agencies which have citations on the upcoming docket.

11–20. Hearing types

All petty-offense violations are either an optional court appearance (O) or a mandatory court appearance (M). The optional Central Violations Bureau Form allows for a predetermined forfeiture of collateral amount to be paid which will close the Central Violations Bureau Form. The hearing type is listed on the petty offense docket between the violation number and the defendant's name. Optional is designated as "O." A mandatory appearance will be shown as an "M." If the officer fails to write the forfeiture amount on the Central Violations Bureau Form, CVB will automatically enter "M" for mandatory appearance. The court will choose to change hearing types from mandatory to optional and indicate the dollar amount that may be forfeited on the docket.

11–21. Forfeiture of collateral on a court docket

Once on the docket, images of the Central Violations Bureau Form(s) and warrant(s) have been mailed to the court, the CVB will email the court if a payment has been made on a Central Violations Bureau Form on the docket. All payments received by CVB are processed daily. Therefore, the CVB will notify the court of any payments received on the docket the next working day.

11–22. Payment by credit card

The CVB can accept payment by credit card for fines to minimize deferred or installment payments for petty offense fines. The U.S. magistrate judge's courtroom deputy will also provide the defendant with a Plastic Card Sale Transaction to complete. The defendant should mail the Plastic Card Sale Transaction to the CVB lockbox facility (Central Violations Bureau, P.O. Box 70939, Charlotte, NC 28272–0939). Please ensure all fields have been completed. A daytime phone number should be used when applicable. The CVB will process the credit card payment when received. If the credit card company denies the use of the card, the CVB will notify the defendant that the charge was denied.

11–23. Payroll deductions

If a court services a military installation, payroll deductions will be used. This allows the fine assessed to be deducted from the defendant's payroll check and deposited to the U.S. Treasury. The information will be provided by the Military Financial Section. Upon receipt of the docket with a disposition code of "PR" or "TR," the CVB will close the case.

11–24. Citations on the docket to be reset

In some cases, additional time is required by the court or the defendant to prepare for the case. The citation will then be reset. The CVB will initially set the cases for the first hearing; thereafter, the court is responsible for all resets. Notification to the defendant of the reset must be made by the court.

11–25. Agency monthly reports

The "Agency Open Index Report" is emailed monthly to each agency. It lists all pending Central Violations Bureau Forms. It will also indicate if the Central Violations Bureau Form has been set for a hearing. In the form of a two-letter code it shows what, if any, action has occurred on the Central Violations Bureau Form. It is the responsibility of each agency to notify the CVB of any changes in personnel. The agency should provide a name, email address, phone, and fax number for each point of contact. The "Agency Closed Index Report" is emailed monthly to the agencies and is similar to the "Agency Open Index Report." It lists all violations closed the previous month, the date the violation was disposed of, and in the form of a two letter-code which indicates the disposition of the case. These reports provide an excellent means of comparing agency records with those of the CVB. Agencies should contact the CVB if there are any discrepancies between the reports.

11–26. Waiver of venue for plea and sentence

Pursuant to Rule 58(c)(2) of the Federal Rules of Criminal Procedure, a defendant will state in writing a wish to plead

guilty or nolo contendere to waive venue and trial in the district where the violation is pending and consent to disposition of the case in a district in which that defendant is present. Unless the defendant thereafter pleads not guilty, the prosecution will be had as if venue were in such district. Notice of the same will be given to the magistrate judge in the district where the violation was originally commenced. The defendant's statement of a desire to plead guilty or nolo contendere is not admissible against the defendant. The original request, made under Rule 58(c)(2) of the Federal Rules of Criminal Procedure, is then forwarded to the court which currently has jurisdiction of the case for transfer. The magistrate judge signs the request and returns the file and the request to the requesting court. A copy of the signed order should be mailed to the CVB. Upon receipt of the original documents, the receiving court will set the case for the next available docket.

11–27. Intra-district transfer

When a Central Violations Bureau Form is transferred from one U.S. magistrate judge to another in the same district, the notice and any other paperwork is mailed directly from the present U.S. magistrate judge to the receiving U.S. magistrate judge. The CVB is notified in writing of this intra-district transfer so system records can correctly reflect the U.S. magistrate judge assigned to the case.

11–28. Voice Case Information System

The Voice Case Information System (VCIS) is available by calling CVB's main number at 1–800–827–2982. The VCIS provides case information over the telephone 24 hours per day. Defendants, agencies, and courts can verify if a payment has been received or a date a citation has been scheduled.

11–29. Central Violations Bureau database search option through email

The CVB has an email program that can be used instead of calling VCIS. It is superior to the VCIS telephone functionality in a number of ways. There is no limit to the number of citations that can be checked and it is able to retrieve the information in less time. There is more information available via email. The response will be via email so the information can be kept electronically for your records. Simply list the citations in an email and send it to search@cvb.uscourts.gov. To use the system, do the following:

a. Compose an email to search@cvb.uscourts.gov. The subject of the email does not matter. The return email will have the same subject as you enter. It is suggested that the user choose something he or she will recognize.

b. Create a list of citations. The list should start with a line containing the word "start" followed by one citation per line. After the last citation add a line containing the word "end." For example—

(1) Start.

(2) A1234567.

(3) B2345678.

(4) C3456.

(5) End.

(6) In this example, searches for citation numbers A1234567, B2345678, and C3456 will be performed against the CVB database.

c. Send your message.

d. Wait for a reply. The reply should return to you within a few minutes of submission.

11–30. Disposition of personnel subject to the Uniform Code of Military Justice

Personnel subject to the UCMJ who pay a fine or forfeit collateral or whose cases are disposed of in accordance with this regulation will not be punished under the provisions of the UCMJ for the same violation. Installation commanders should establish policies on how to refer Army personnel to the U.S. magistrate for disposition when the violator's conduct constitutes a misdemeanor within the magistrate's jurisdiction and is also a violation of the UCMJ. Such policies must be consistent with directives of higher headquarters and coordinated through installation SJAs and with local U.S. magistrates or U.S. District Courts.

11–31. Disposition of juvenile offenders

Juveniles are not subject to the jurisdiction of U.S. magistrates or U.S. District Courts without a certification by the U.S. Attorney General that the state juvenile court lacks jurisdiction, refuses to assume jurisdiction, or does not have adequate programs and services available (under 18 USC 5032). Therefore, coordination should be made with local juvenile authorities concerning the disposition of offenses committed by juveniles on Army installations. Coordination will also be made with the appropriate Juvenile Disciplinary Advisory Council, which will also have the authority to dispose of offenses committed by juveniles.

Chapter 12 National Crime Information Center Policy

12-1. Authority

The authority for Army LE agencies to access CJIS, NCIC, and NLETS is based on this regulation, user agreements between the installation LE activity and the respective State government's CTA, and issuance of an originating agency identifier (ORI). All transactions must be according to the standards of this regulation, the NCIC Operating Manual, State government user manuals, and State user agreements. In instances where there will be a conflict in standards, the strictest policy interpretation will apply.

12-2. Standards

The following standards must be followed in operating terminals:

- a. The NCIC use is limited to authorized criminal justice purposes, such as stolen vehicle checks or wants and warrants. Subject to FBI regulations and policy, NCIC checks of visitors to a military installation may be authorized by the installation or garrison commander in accordance with DOD 5200.08-R and DODI 5200.08. Visitors to Army installations are non-DOD affiliated personnel.
- b. Dissemination of information is based on an official need to know.
- c. Only trained and authorized personnel will operate terminals.
- d. An Army agency queried over the NCIC must respond within 10 minutes for a priority-1 (urgent) hit confirmation and within 1 hour for a priority-2 (routine) hit confirmation.
- e. Required NCIC documentation and State-written documentation must be prepared and retained for audit by the NCIC or State CTA.
- f. Army LE agencies will not use DOJ Joint Automated Book System accounts to directly interface with CJIS.
- g. Only personnel in the Latent Print Division of the USACIL will submit or receive IAFIS transactions involving latent finger or palm prints.

12-3. Authorized access

- a. The NCIC terminal operators are authorized access to files maintained in the NCIC in the performance of their official duties:
- b. Participation in other Federal, State, and local police information systems is authorized.

12-4. Reports of positive urinalysis-test results entered into the National Instant Checks System database though National Crime Information Center

The NICS Improvement Amendment Act of 2007 creates independent statutory obligation for Federal agencies to report records identifying prohibited persons to the U.S. Attorney General. Army LE is required to report positive drug urinalysis tests to the NICS under the authority of 18 USC 922 (The Brady Handgun Violence Prevention Act of 1993) for the following:

- a. Unlawful users, in accordance with 18 USC 922(g)(3) and 27 CFR 478.11. It is unlawful for any person who is an unlawful user of, or addicted to, any controlled substance as defined in 21 USC 802 (The Controlled Substance Act) section 102, to purchase weapons.
 - (1) Inference of current use may be drawn from evidence of recent use or possession of a controlled substance, or a pattern of use or possession that reasonably covers the present time such as—
 - (a) Conviction for use or possession of a controlled substance within the past year.
 - (b) Multiple arrests for such offenses within past 5 years if most recent arrest occurred within past year, or
 - (c) Person found through a drug test to use a controlled substance unlawfully, provided test was administered within past year.
 - (2) Sentence coming soon.
- b. Upon being notified of a positive urinalysis test administered within the last year, LE staff will enter the information into the NICS database using their NCIC terminal. (States that do not have the capability to enter NICS information are exempt until a change to their operating systems and/or funding is provided.) An entry into the NICS index requires, at a minimum, the following fields to be populated:
 - (1) NICS message field "EDP."
 - (2) Name.
 - (3) Sex.
 - (4) PCA – prohibited category code (enter the code C).
 - (5) Date of birth.
 - (6) ARI – agency records identifier (MP case number).
- c. The entry requires that an expiration date be added. The expiration date will be 1 year from the positive urinalysis date. For example, for a positive test date of "20100123," the expiration date will be "20110123."

d. The NICS database will automatically purge the information on the expiration date.

Chapter 13 National Crime Information Center Procedures

13-1. Requesting an originating agency identifier

a. To be considered for participation and assignment of an ORI, an activity must meet the standards of the NCIC and the State CTA.

b. Requests for participation are initiated by the installation PM or DES and submitted to the garrison commander; requests are then forwarded through the regional IMCOM office or ACOM, ASCC, DRU commander. The regional IMCOM office will forward their requests to the HQDA IMCOM and to the Director, USACRC for a decision. The ACOM, ASCC, and DRU commanders will forward their requests to the Director, USACRC for a decision. The Director, USACRC will disapprove requests that do not meet the criteria of this regulation, NCIC, or state eligibility requirements. See figures 13-1 and 13-2, below, for an example of a request for an ORI.



DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

(office symbol)(date)

MEMORANDUM THRU

FOR DIRECTOR, U.S. ARMY CRIME RECORDS CENTER (CICR-ZA), 6010 6th Street, Fort Belvoir, VA 22060

SUBJECT: Request for Originating Agency Identifier (ORI)

1. Request an ORI number be assigned to the provost marshal office on this installation.
2. This request meets the criteria of AR 190-27, Army Participation in the National Crime Information Center (NCIC). The ORI number will be used to enter records into and query the NCIC, with the exception of the interstate identification index file.
3. Funding for leasing or purchasing equipment for connection to the State Control Terminal Agency (CTA) is available. On approval of this request, a users' agreement will be signed with the CTA. Use of the ORI will be limited to criminal justice purposes.

(garrison commander signature)

Figure 13-1. Sample request from a regional office of the Installation Management Command to obtain an originating agency identifier



DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

(office symbol)

(date)

MEMORANDUM FOR DIRECTOR, U.S. ARMY CRIME RECORDS CENTER (CICR-ZA),
27130 TELEGRAPH ROAD, QUANTICO, VA 22134-2253

SUBJECT: Request for Originating Agency Identifier (ORI)

1. Request assignment of an ORI number for the Provost Marshal Office on this installation.
2. This request meets the criteria of AR 190-45, Military Police Law Enforcement Reporting. The ORI number will be used to enter records into and query the NCIC, with the exception of the interstate identification index file.
3. Funding is available for leasing or purchasing equipment required for connection to the State Control Terminal Agency (CTA). Upon approval of this request, a user agreement will be signed with the CTA. The ORI will only be used for criminal justice purposes.

(ACOM, ASCC, or DRU garrison commander
signature)

Figure 13-2. Sample request—from an Army command, Army service component command, or direct reporting unit—to obtain an originating agency identifier

13-2. Suspension or revocation

- a. The NCIC and State CTAs have the authority to suspend or revoke an Army terminal's access to files when operating policies are not correctly followed.
- b. Notification of serious violations, suspension, or revocation from the use of NCIC and State government terminals and NCIC files will be immediately reported directly to the Director, USACRC's Federal service coordinator by the most expeditious means. The Federal service coordinator will review the circumstances and effect immediate coordination to resolve issues.
- c. When notified of a serious violation, the installation PM or DES will take corrective action required by the NCIC or State government's CTA.

13-3. Entry

- a. Entry messages place a new record in the NCIC using the ORI assigned to the agency. Procedures for entering a new record are explained in each file of the NCIC Operating Manual.
 - (1) The installation PMs or DESs within the CONUS, as well as Alaska, and Hawaii will enter stolen or missing government property valued at \$500 or more and having a unique manufacturer assigned serial number. All Government or privately owned weapons reported lost, stolen, or recovered will be entered into the NCIC gun file, regardless of value.
 - (2) Director, USACRC, enters stolen property and gun reports for PM or DES offices in overseas areas.
- b. LE activities not located on an Army installation or having access to a terminal will enter into a written

agreement with an installation PM or DES to have the installation PMO or DES enter records and act as the ORI holder. Figure 13–3, below, is an example of an ORI holder agreement.

Holder of Record Agreement

This agreement made this 3rd day of January 2004, by and between the Army Corps of Engineers, Northwestern District, owner of record, and Office of the Provost Marshal, Fort Lewis, WA, holder of record, is entered into for the purpose of making the holder of record responsible for entering and maintaining records in the NCIC/Washington State system for the owner of record, under the following conditions:

1. The holder of record will be responsible for updating and canceling all records maintained in the NCIC/Washington State system for the owner of record.
2. The holder of record will comply with all NCIC requirements.
3. The holder of record will remove all records from the file belonging to the owner of record, in compliance with NCIC requirements.
4. The holder of record will validate any record of the owner of record in accordance with Washington State requirements.
5. The owner of record will notify the holder of record immediately when any record affected by this agreement is to be canceled, cleared, or modified.
6. The owner of record will provide complete supporting documentation to the holder of record prior to requesting any entries be made.

This agreement will remain in effect as long as:

1. The holder of record is a member of the NCIC/Washington State system.
2. The owner of record does not become an NCIC/Washington State system member.

The agency head of either agency shall give 30 days' notice to the other, in writing, of its intent to withdraw from this agreement. Should the agencies withdraw from this agreement, the holder of the record will remove all records for the owner of record from the files and notify the owner of record, in writing, that this has been accomplished. The State will be sent a copy of this notice:

In witness wherefore, the parties signatory hereto have executed this agreement as the day and year first above written in accordance with the authority granted them by law and have provided a copy of the same to the Department of State Police.

<u>Xxxxx Xxxxx</u> (typed name) Owner of Record	<u>Xxxxx Xxxxx</u> (typed name) Holder of Record
<u>(Xxxx's signature here)</u> Signature	<u>(Xxxx's signature here)</u> Signature
<u>(insert name of state terminal agency here)</u> Control Terminal Agency	

Figure 13–3. Sample of an originating agency identifier holder agreement

13-4. Modification

Modification messages are used to add, delete, or change a portion of data that is part of the NCIC entry. An entering agency will modify a record while it is in an active status following file procedures in the NCIC Operating Manual.

13-5. Cancellation

Canceling an NCIC entry removes the entire record from the NCIC. A record must be canceled by the entering ORI when it is determined to be invalid.

13-6. Validation

The NCIC periodically prepares a listing of records on file for validation by system users. Each State CTA and Federal service coordinator receives a letter explaining the records on the validation list, the order in which records are listed, and general procedures for validating the records. Army participants must validate their records and respond to the State CTA. Failure to comply with validation procedures could result in the record being deleted or administrative action taken against the entering agency.

13-7. Army participation in Criminal Justice Information System

a. Programs consolidated under the CJIS Division included the NCIC, UCR, and Fingerprint Identification Program. In addition, responsibilities include the IAFIS, NCIC 2000, and the NIBRS.

b. The installation PM's or DES's procedures for submitting data to the UCR, IAFIS, and NIBRS are explained paragraph 4-10.

c. The purchase of IAFIS equipment must be coordinated and approved by the Installation Management Agency, or the ACOM, ASCC, DRU commanders, and the Director, USACRC. This will ensure that all IAFIS devices are compatible and that the Director, USACRC, properly submits all fingerprint submissions to IAFIS and the criminal history file of the NCIC.

Appendix A References

Section I Required Publications

Unless otherwise stated, all publications are available at <http://www.apd.army.mil/>. Department of Defense regulations are available at <http://www.dtic.mil/>. The U.S. Code is available at <http://www.gpo.gov/fdsys/>.

AR 25–55

The Department of the Army Freedom of Information Act Program (Cited in para 2–1*a*.)

AR 25–400–2

The Army Records Information Management System (ARIMS) (Cited in para 1–4*a*(2).)

AR 27–10

Military Justice (Cited in para 2–7*b*(2).)

AR 190–9

Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies (Cited in para 2–9*c*.)

AR 195–2

Criminal Investigation Activities (Cited in para 2–5*a*.)

AR 340–21

The Army Privacy Program (Cited in para 2–1*a*.)

AR 360–1

The Army Public Affairs Program (Cited in para 3–1*a*.)

AR 380–5

Department of the Army Information Security Program (Cited in para 2–2*a*.)

AR 380–10

Foreign Disclosure and Contacts with Foreign Representatives (Cited in para 3–8*b*.)

AR 380–13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations (Cited in para 2–5*c*.)

AR 381–10

U.S. Army Intelligence Activities (Cited in para 8–3*x*.)

AR 381–12

Threat Awareness and Reporting Program (Cited in para 1–4*a*(6).)

AR 525–13

Antiterrorism (Cited in para 8–7*g*(3).)

AR 600–20

Army Command Policy (Cited in para 4–15.)

AR 600–37

Unfavorable Information (Cited in para 3–3*a*.)

AR 600–63

Army Health Promotion (Cited in para 2–1*a*.)

AR 600–85

The Army Substance Abuse Program (Cited in para 3–3*a*.)

AR 608–18

The Army Family Advocacy Program (Cited in para 3–9a.)

AR 630–10

Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings (Cited in para 4–11a(2).)

AR 710–2

Supply Policy Below the National Level (Cited in para 8–3d(2).)

CJCSM 3150.03D

Joint Reporting Structure Event and Incident Reports (Cited in para 1–4b(10).) (This classified issuance is available to authorized individuals at <http://www.intelink.sgov.gov/sites/jointstaff>)

DA Pam 600–24

Health Promotion, Risk Reduction, and Suicide Prevention (Cited in para 2–1a.)

DOD 4160.21–M

Defense Materiel Disposition Manual (Cited in paras 4–14, 4–14c.)

DOD 6025.18–R

DOD Health Information Privacy Regulation (Cited in para 8–1g.)

DODI 5505.14

Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations (incorporating change 1, April 24, 2012) (Cited in para 2–8a.)

Federal Rules of Criminal Procedure, Rule 58

Petty Offenses and Other Misdemeanors (Cited in para 10–4a.)

Federal Rules of Criminal Procedure, Rule 58(c)(2)

Additional Procedures in Certain Petty Offense Cases: Waiving Venue (Cited in para 11–26.)

National Crime Information Center

National Crime Information Center Operating Manual (Cited in para 12–1.) (This manual may be obtained from the FBI, Washington, DC 20535.)

UCMJ, Article 112a

Wrongful use, possession, etc., of controlled substances (Cited in paras 2–8e(1), table 4–1.)

18 USC 13

Laws of states adopted for areas within Federal jurisdiction (Cited in table 4–1, para B–2b(1), and glossary section II.)

50 USC 1801 et seq

The Foreign Intelligence Surveillance Act (Cited in para 8–7h(2)(b).)

Section II**Related Publications**

A related publication is merely a source of additional information. The user does not have to read it to understand this publication. Unless otherwise stated, all publications are available at: <http://www.apd.army.mil/>. Department of Defense regulations are available at: <http://www.dtic.mil/>. The U.S. Code, the Federal Register, the Code of Federal Regulations, acts of Congress, and public laws are available at: <http://www.gpo.gov/fdsys/>. Executive orders are available at: http://www.archives.gov/federal_register/executive_orders/disposition_tables.html

AD 2011–17

Self-Reporting by Officers and Senior Enlisted Members of Criminal Convictions.

AD 2013–06

Providing Specified Law Enforcement Information to Commanders of Newly Assigned Soldiers

AR 15-1

Committee Management

AR 15-6

Procedures for Investigating Officers and Boards of Officers

AR 20-1

Inspector General Activities and Procedures

AR 25-1

Army Knowledge Management and Information Technology

AR 27-20

Claims

AR 27-40

Litigation

AR 40-61

Medical Logistics Policies

AR 40-66

Medical Record Administration and Health Care Documentation

AR 190-5/OPNAV 11200.5D/AFI 31-218(I)/MCO 5110.1D/DLAR 5720.1

Motor Vehicle Traffic Supervision

AR 190-9

Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies

AR 190-11

Physical Security of Arms, Ammunition, and Explosives

AR 190-30

Military Police Investigations

AR 190-47

The Army Corrections System

AR 190-53

Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 195-5

Evidence Procedures

AR 380-67

Personnel Security Program

AR 381-20

The Army Counterintelligence Program

AR 600-8-2

Suspension of Favorable Personnel Actions (Flags)

AR 600-85

Army Substance Abuse Program

ATTP 3-39.10

Law and Order Operations

7 CFR 331

Agriculture: Possession, use, and transfer of select agents and toxins

9 CFR 121

Animals and Animal Products: Possession, use, and transfer of select agents and toxins

27 CFR 478.11

Alcohol, Tobacco Products and Firearms: Meaning of terms

32 CFR 505.5(i)(2)(i)

Procedures for denying or limiting an individual's right to access or amendment and the role of the Denial Authority

36 CFR 330

Regulation of law enforcement services contracts at civil works water resource projects administered by the Chief of Engineers

42 CFR 73

Select agents and toxins

DOD 5200.08

Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)

DOD 5200.08-R

Physical Security Program (April 9, 2007, as amended)

DOD 5240.1-R

Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons

DOD 5400.7-R

DOD Freedom of Information Act Program

DOD 8320.02-G

Guidance for Implementing Net-Centric Data Sharing

DODD 1030.01

Victim and Witness Assistance

DODD 5240.1

DOD Intelligence Activities

DODI 1000.30

Reduction of Social Security Number (SSN) Use Within DoD

DODI 1030.2

Victim and Witness Assistance Procedures

DODI 1325.07

Administration of Military Correctional Facilities and Clemency and Parole Authority

DODI 5505.11

Fingerprint Card and Final Disposition Report Submission Requirements

DODI 5505.14

Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders

DODI 5525.11

Criminal Jurisdiction Over Civilians Employed by or Accompanying the Army Forces Outside the United States, Certain Service Members, and Former Service Members

DODI 7730.47

Defense Incident-Based Reporting System (DIBRS)

DTM 08–035

Self-Reporting by Officers and Senior Enlisted Members of Criminal Convictions

DTM 09–012

Interim Policy Guidance for DOD Physical Access Control

DTM 10–018

Law Enforcement Reporting of Suspicious Activity, dated 1 October 2010

EO 13478

Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers

EO 12333

United States Intelligence Activities

Federal Rules of Criminal Procedure, Rule 6(e)

Recording and Disclosing the Proceedings (Available at: <http://www.uscourts.gov/RulesAndPolicies/rules/current-rules.aspx>)

Federal Rules of Criminal Procedure, Rule 58(c)(2)

Additional Procedures in Certain Petty Cases: Waiving Venue

33 Federal Register 5495

The National Guidelines for Sex Offender Registration and Notification, Final Guidelines

73 Federal Register 38030–38050

The National Guidelines for Sex Offender Registration and Notification

Joint Publication 6–0

Joint Communications System Available at: http://www.dtic.mil/doctrine/new_pubs/jointpub_communications.htm

PL 106–65

National Defense Authorization Act for Fiscal Year 2000

PL 106–523

Military Extraterritorial Jurisdiction Act of 2000

PL 108–375

Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005

PL 110–53

Implementing Recommendations of the 9/11 Commission Act of 2007

HR 2640

NICS Improvement Amendments Act of 2007

RCM 305(h)(2)(c)

Pretrial confinement, 72-hour memorandum

RCM 307

Preferral of charges

UCMJ, Article 15

Commanding officer's non-judicial punishment

UCMJ, Article 90

Assaulting or willfully disobeying superior commissioned officer

UCMJ, Article 92

Failure to obey order or regulation

5 USC 552

The Freedom of Information Act

5 USC 552a

The Privacy Act of 1974

5 USC 2951

Reports to the Office of Personnel Management

6 USC 1104

Immunity for reports of suspected terrorist activity or suspicious behavior and response

10 USC 301

Definitions

10 USC 1561a

Civilian orders of protection: force and effect on military installations

10 USC 2671

Military reservations and facilities: hunting, fishing, and trapping

15 USC 2605

Toxic Substance Control Act

16 USC 668

The Bald Eagle Protection Act

16 USC 703

The Migratory Bird Treaty Act

16 USC 718

The Migratory Bird Hunting Stamp Act

16 USC 3372

The Lacey Act

18 USC 922

The Brady Handgun Violence Prevention Act of 1993, Revised Statute

18 USC 1382

Entering military, naval, or Coast Guard property

18 USC 5032

Delinquency proceedings in district courts; transfer for criminal prosecution

21 USC 13

The Comprehensive Drug Abuse Prevention and Control Act of 1970

21 USC 802

Controlled Substance Act

28 USC 534

The Uniform Federal Crime Reporting Act

29 USC 655

Occupational Safety and Health Act of 1970

33 USC 1251

Water Pollution Control Act

42 USC 300f et seq

Safe Drinking Water Act

42 USC 14132

Index to Facilitate Law Enforcement Exchange of DNA Identification Information

42 USC 4321

National Environmental Policy Act

42 USC 6901

Hazardous Waste Control Act

42 USC 7401

Clean Air Act

42 USC 9601

Comprehensive Environmental Response, Compensation, and Liability Act

42 USC 10601

The Victim Rights and Restitution Act

42 USC 14135a(a)(1)(a)

Collection and Use of DNA Identification Information from Certain Federal Offenders: Collection of DNA Samples from Individuals in Custody

42 USC 16901

The Sex Offender Registration and Notification Act

42 USC 16911(5)(B)

Relevant definitions, including Amie Zyla expansion of sex offender definition and expanded inclusion of child predators: Foreign convictions

U.S. Supreme Court Case 425 U.S. 252

Middendorf v. Henry (Available at: <http://supreme.justia.com/cases/federal/us/425/25/>)

Section III

Prescribed Forms

Unless otherwise indicated, DA forms are available on the APD Web site at <http://www.apd.army.mil> and DD forms are available on the OSD Web site at <http://www.dtic.mil/whs/directives/infomgt/forms/>.

DA Form 2823

Sworn Statement (Prescribed in paras 7–10, 7–11.)

DA Form 3945

Military Police Radio Log (Prescribed in para 7–13.)

DA Form 3946

Military Police Traffic Accident Report (Prescribed in paras 4–2, 7–14.)

DA Form 4833

Commander's Report of Disciplinary or Administrative Action (Prescribed in paras 4–7, 4–8.)

DD Form 460

Provisional Pass (Prescribed in paras 4–11, 7–2.)

DD Form 2701

Initial Information for Victims and Witnesses of Crime (Prescribed in paras 6–3, 6–4.)

FBI Form FD 249

CJIS Fingerprint Supply/Requisition Form (Prescribed in para 4–10.) (Obtain directly from FBI.)

FBI Form R–84

Final Disposition Report (Prescribed in para 4–10.) (Obtain directly from FBI.)

Section IV**Referenced Forms**

Unless otherwise indicated, DA forms are available on the APD Web site, at <http://www.apd.army.mil> and DD forms are available on the OSD Web site, at <http://www.dtic.mil/whs/directives/infomgt/forms/>.

DA Form 190–45–SG

Army Law Enforcement Reporting and Tracking System (ALERTS) (Available through the Provost Marshal General.)

DA Form 1602

Civilian Identification (Available through normal forms supply channels.)

DA Form 2028

Recommended Changes to Publications and Blank Forms

DA Form 2804

Crime Records Data Reference

DA Form 3626

Vehicle Registration/Driver Record

DA Form 3881

Rights Warning Procedure/Waiver Certificate

DA Form 4002

Evidence/Property Tag (Available through normal forms supply channels.)

DA Form 4137

Evidence/Property Custody Document

DA Form 4187

Personnel Action

DA Form 7630

Department of the Army Law Enforcement Escort Credential (S&I HQDA, OPMG (DAPM–MPO–LE), 2800 Army Pentagon, Washington, DC 20310–2800.)

DD Form 553

Deserter/Absentee Wanted by the Armed Forces

DD Form 616

Report of Return of Absentee

DD Form 1173

Uniformed Services Identification and Privilege Card (Available through normal forms supply channels.)

DD Form 1408

Armed Forces Traffic Ticket (Available through normal forms supply channels.)

DD Form 1920

Alcohol Incident Report

DD Form 2707

Confinement Order

DD Form 2708

Receipt for Pre Trial/Post Trial Prisoner or Detained Person

DD Form 2791

Notice of Release/Acknowledgement of Convicted Sex Offender Registration Requirements

DD Form 2873

Military Protective Order

DD Form 2977

Deliberate Risk Assessment Worksheet

Central Violations Bureau (CVB) Form

United States District Court Violation Notice (Obtain directly from the CVB at <http://www.cvb.uscourts.gov/>.)

Appendix B

Contact information and mailing addresses for serious-incident reports

Commonly used information addresses on SIRs are listed below.

B-1. Army Materiel Command

MSG: CDR, USAMC Fort Belvoir, VA (AM-CS)
Fax: 703-806-9280 DSN: 656-9280

B-2. Army watch

MSG: armywatch.aoc@us.army.mil

B-3. Defense Intelligence Agency

MSG: DIA, Washington, DC (OS-1/JSO)

B-4. Eighth United States Army

MSG: CDR, USAEIGHT, Seoul, KOR (PMJ)
FAX: 011-822-7918 DSN: 738-6290

B-5. Forces Command

MSG: CDR, FORSCOM, Fort McPherson, GA (AFPM)
Fax: 404-464-5938 DSN: 367-5938

B-6. Headquarters, Department of the Army, Office of the Provost Marshal General

(DAPM-MPP) MSG: DA Washington, DC (OPMG-LE)
email: mpops@conus.army.mil
Fax: 703-693-6580 DSN: 223-4243

B-7. Installation Management Command

MSG: imcomopscenter@hqda.army.mil
email: usarmy.jbsa.imcom-hg.list.operations-center-dl@mail.mil
Fax: 703-602-1703 DSN: 332-1703

B-8. National Guard Bureau

MSG: CNGB, Washington, DC (NGBZA)

B-9. Surface Deployment and Distribution Command

MSG: CDR, MTMC, Falls Church, VA (MTSS)
Fax: 703-756-0547 DSN: 289-0547

B-10. Training and Doctrine Command

MSG: CDR, TRADOC, Fort Monroe, VA (ATTG-J)
Fax: 757-788-3504 DSN: 680-3504

B-11. U.S. Army Community and Family Support Center

MSG: CDR, USACFSC, Alexandria, VA (CFSC-FSC)

B-12. U.S. Army Criminal Investigation Command

MSG: CDR, USACIDC, Fort Belvoir, VA (CIOP-ZA)
FAX: 703-806-0307

B-13. U.S. Army Europe

MSG: CINCUSAREUR, Heidelberg, GE (AEAPM)
Fax: 011-49-621-730-7324 DSN: 8-314-381-7324

B-14. U.S. Army Information Systems Command

MSG: CDR, USAISC, Fort Huachuca, AZ (ASIS-S)
Fax: 602-538-8787 DSN: 879-8787

B-15. U.S. Army Medical Command

MSG: CDR, USAMEDCOM, Fort Sam Houston, TX (MCOP-O-PM)

Fax: 210-221-6055 DSN: 471-6055

B-16. U.S. Army Military Police School

MSG: COMDT, MPSCH, Fort Leonard Wood, MO (ATZN-MP-Z)

B-17. U.S. Army Reserve

MSG: CDR, USARC, Fort McPherson, GA (AFRC-CG)

B-18. U.S. Army Pacific

MSG: CDR, USARPAC, Fort Shafter, HI (APPM)

Fax: 808-438-9313 DSN: 315-9313

B-19. U.S. Secret Service

MSG: U.S. Secret Service, Washington, DC

Appendix C

Offense codes for Army investigations

C-1. Alphanumeric codes

Each offense code describes, as nearly as possible, the complaint or offense by using an alphanumeric code. This list will be amended from time to time, based on new reporting requirements mandated by legislation or administrative procedures. The IMCOM, ACOM, ASCC, and DRU commanders, and the installation PMOs and DESs, will be notified by special letters of instruction issued in numerical order from the OPMG when additions or deletions are made to the list.

C-2. Reporting offenses

The DA Form 190-45-SG, also known as ALERTS, will be used for all reporting requirements.

Table C-1
Offense code list

Offense code	Description	UCMJ Article	United States Code	CRC reportable
3A1	Traffic fatality (noncriminal)	No criminal act		Yes
3B1	Driving under the influence - with personal injury	Article 111		Yes
3B2	Driving under the influence - without personal injury	Article 111		Yes
3C1	Fleeing the scene of accident	Article 134		Yes
3C2	Traffic offenses - accident	No criminal act		No
3C3	Traffic violations - other	Article 134		Yes
3C4	Careless or reckless driving - personal injury	Article 1111		Yes
3C5	Careless or reckless driving - other cases	Article 134		Yes
3C6	Traffic accident - other cases - none	Article 134		No
3C7	Traffic Offenses - Alcohol/Drug Related	Article 134		No
3D2	Registration Violation - Vehicle	Article 134		No
3D3	Registration Violation - Fish/Game	Article 134		No
3D4	Other Registration Violations (Weapon, etc.)	Article 134		No
3E2	Weapons Violations - Carrying/Possessing/Concealing	Article 134		Yes
3E3	Other Weapons Matters	Article 134	18 USC 930	No
3E4	Discharge Firearm - Neglect/Willful	Article 134		Yes
3F2	Escape from Custody	Article 95		Yes
3F3	Escape from Pretrial Confinement	Article 95	18 USC 751	Yes
3F4	Escape from Post-trial Confinement	Article 95	18 USC 751	Yes
3F5	Escape from Correctional Custody	Article 95		Yes
3F6	Breach of Correctional Custody	Article 95		Yes
3G2	Release Prisoner Without Authority	Article 96	18 USC 751	Yes
3G3	Allow Escape by Neglect	Article 96	18 USC 755	Yes
3G4	Allow Escape by Design	Article 96	18 USC 755	Yes
3G5	Allowing Prisoner to do Unauthorized Act	Article 134		Yes
3H2	Resisting Apprehension - Military	Article 95	18 USC 111	Yes
3H3	Resisting Arrest - Civilian	Article 95	18 USC 111	Yes
3H4	Break Arrest	Article 95	18 USC 751	Yes
3H5	Break Quarantine	Article 134		Yes
3H6	Break Restriction	Article 134		Yes
3H7	Unlawful Detention	Article 97		Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
3H8	Parole Violation	Article 134		Yes
3J1	Desertion	Article 85		Yes
3J2	AWOL	Article 86		Yes*
3J3	Failure to Go to Place of Duty	Article 86		Yes
3J4	Goes From Place of Duty	Article 86		Yes
3J5	Abandoning Watch or Guard - No Intent	Article 86		Yes
3J6	Abandoning Watch or Guard - Intent to Abandon	Article 86		Yes
3J7	Abandoning Watch or Guard - Intent to Avoid Maneuvers	Article 86		Yes
3K1	Sentinel Misbehave In War	Article 113		Yes
3K2	Sentinel Misconduct	Article 113		Yes
3K3	Missing Movement - by Design	Article 87		Yes
3K4	Missing Movement - by Neglect	Article 87		Yes
3L1	Malingering During Time of War	Article 115		Yes
3L2	Malingering - Other	Article 115		Yes
3L3	Injury Self During Time of War	Article 115		Yes
3L4	Injury Self - Not Time of War	Article 115		Yes
3L5	Straggling	Article 134		Yes
3M1	Conduct Unbecoming Officer	Article 133		Yes
3M2	Military Offenses - Contempt/Disrespect/Disobey	Article 88		Yes
3M3	Contempt Towards Official	Article 88		Yes
3M4	Disrespect Towards Superior Commissioned Officer	Article 89		Yes
3M5	Insubordinate Conduct - Disrespect	Article 91		Yes
3M6	Disobeying/Insubordinate Conduct	Article 90		Yes
3M7	Failure to Obey General Order	Article 92		Yes
3M8	Derelection of Duties - Willful/Neglect	Article 92		Yes
3M9	Cruelty of Subordinates	Article 93		Yes
3N1	Failure to Enforce Procedural Rule	Article 98		Yes
3N2	Wrongful Interferences W/Admin Proceedings	Article 134		Yes
3N3	Alter/remove public record	Article 134	18 USC 2071	Yes
3N4	Refuse to Testify	Article 134		Yes
3P1	Sentinel Misconduct	Article 113		Yes
3P2	Mutiny	Article 94	18 USC 2387	Yes
3P3	Seduction	Article 94	18 USC 2384	Yes
3Q1	Misconduct Before Enemy	Article 99		Yes
3Q2	Strike Flag Before Enemy	Article 100		Yes
3Q3	Hazard Vessel - Willful/Neglect	Article 110		Yes
3Q4	Jump Vessel	Article 134		Yes
3Q5	Improper Use of Countersign	Article 101		Yes
3Q6	Forcing Safeguard	Article 102		Yes
3R1	Drunk in Public	Article 134		No

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
3R2	Drunk on Duty	Article 112		Yes
3R3	Drunk and Unable to Perform Duties	Article 134		No
3R4	Drink Liquor with Prisoner	Article 134		No
3R5	Drunk prisoner	Article 134		No
3R6	Disorderly Conduct	Article 134		No
3R7	Drunk and Disorderly	Article 92		Yes*
3S1	Violation of a Military Protective Order	Article 92		Yes
3S2	Violation of a Civilian Protective Order	Article 92		Yes
3T1	Fraternization	Article 134		Yes
3T2	Unlawful Cohabitation	Article 134		No
3U1	Disloyal Statement	Article 134	18 USC 792	Yes
Drug Crimes				
Offense Code	Description	UCMJ code	United States Code	CRC reportable
4A	Opiates (for example, Heroin, Morphine)	Article 112a	21 USC 844	Yes
4A1	Wrongful Smuggling of Opiates	Article 112a	21 USC 844	Yes
4A2	Distribution of Opiates	Article 112a	21 USC 841	Yes
4A3	Wrongful Possession of Opiates	Article 112a	21 USC 844	Yes
4A4A	Wrongful Use of Opiates - Detected by Urinalysis	Article 112a	21 USC 844	Yes
4A4B	Wrongful Use of Opiates - Not Detected by Urinalysis	Article 112a	21 USC 844	Yes
4A5	Grow/Manufacture Opiates W/Intent to Distribute	Article 112a	21 USC 841	Yes
4A6	Wrongfully Grow/Manufacture of Opiates	Article 112a	21 USC 841	Yes
4A7	Possession of Opiates W/Intent to Distribute	Article 112a	21 USC 841	Yes
4A8	Wrongful Introduction of Opiates	Article 112a	21 USC 844	Yes
4A9	Introduction of Opiates W/Intent to Distribute	Article 112a	21 USC 841	Yes
4B	Marijuana			
4B1	Wrongful Smuggling of Marijuana	Article 112a	21 USC 844	Yes
4B2	Distribution of Marijuana	Article 112a	21 USC 841	Yes
4B3	Wrongful Possession of Marijuana	Article 112a	21 USC 841	Yes
4B4A	Wrongful Use of Marijuana - Detected By Urinalysis	Article 112a	21 USC 844	Yes
4B4B	Wrongful Use of Marijuana - Not Detected By Urinalysis	Article 112a	21 USC 844	Yes
4B5	Grow/Manufacture Marijuana W/Intent to Distribute	Article 112a	21 USC 841	Yes
4B6	Wrongfully Grow/Manufacture of Marijuana	Article 112a	21 USC 841	Yes
4B7	Possession of Marijuana W/Intent to Distribute	Article 112a	21 USC 841	Yes
4B8	Wrongful Introduction of Marijuana	Article 112a	21 USC 844	Yes
4B9	Introduction of Marijuana W/Intent to Distribute	Article 112a	21 USC 841	Yes
4C	Cocaine			
4C1	Wrongful Smuggling of Cocaine	Article 112a	21 USC 844	Yes
4C2	Distribution of Cocaine		841	Yes
4C3	Wrongful Possession of Cocaine	Article 112a	21 USC 844	Yes
4C4A	Wrongful Use of Cocaine - Detected By Urinalysis	Article 112a	21 USC 844	Yes
4C4B	Wrongful Use of Cocaine - Not Detected by Urinalysis	Article 112a	21 USC 844	Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
4C5	Grow/Manufacture Cocaine W/Intent to Distribute	Article 112a	21 USC 841	Yes
4C6	Wrongfully Grow/Manufacture of Cocaine	Article 112a	21 USC 841	Yes
4C7	Possession of Cocaine W/Intent to Distribute	112a	21 USC 841	Yes
4C8	Wrongful Introduction of Cocaine			Yes
4C9	Introduction of Cocaine W/Intent to Distribute			Yes
4D	Hallucinogens (for example, Lysergic Acid Diethylamide (LSD), Phencyclidine (PCP))			Yes
4D1	Wrongful Smuggling of Hallucinogens			Yes
4D2	Distribution of Hallucinogens			Yes
4D3	Wrongful Possession of Hallucinogens	112a	21 USC 844	Yes
4D4A	Wrongful Use of Hallucinogens - Detected by Urinalysis	112a	21 USC 844	Yes
4D4B	Wrongful Use of Hallucinogens - Not Detected by Urinalysis	112a	21 USC 844	Yes
4D5	Grow/Manufacture Hallucinogens W/Intent to Distribute	112a	21 USC 841	Yes
4D6	Wrongfully Grow/Manufacture of Hallucinogens	112a	21 USC 841	Yes
4D7	Possession of Hallucinogens W/Intent to Distribute	112a	21 USC 841	Yes
4D8	Wrongful Introduction of Hallucinogens	112a	21 USC 844	Yes
4D9	Introduction of Hallucinogens W/Intent to Distribute	112a	21 USC 841	Yes
4E	Anabolic Steroids			
4E1	Wrongful Smuggling of Anabolic Steroids		21 USC 844	Yes
4E2	Distribution of Anabolic Steroids		21 USC 841	Yes
4E3	Wrongful Possession of Anabolic Steroids		21 USC 844	Yes
4E4A	Wrongful Use of Anabolic Steroids - Detected by Urinalysis		21 USC 844	Yes
4E4B	Wrongful Use of Anabolic Steroids - Not Detected by Urinalysis		21 USC 844	Yes
4E7	Possession of Anabolic Steroids W/Intent to Distribute		21 USC 841	Yes
4E8	Wrongful Introduction of Anabolic Steroids		21 USC 844	Yes
4E9	Introduction of Anabolic Steroids W/Intent to Distribute		21 USC 841	Yes
4F	Synthetic Drugs (Identified as Scheduled)			
4F1	Wrongful Smuggling of Synthetic Drugs (that is, Spice and Bath Salts)	112a	21 USC 844	Yes
4F2	Distribution of Synthetic Drugs	112a	21 USC 841	Yes
4F3	Wrongful Possession of Synthetic Drugs	112a	21 USC 844	Yes
4F4A	Wrongful Use of Synthetic Drugs - Detected by Urinalysis	112a	21 USC 844	Yes
4F4B	Wrongful Use of Synthetic Drugs - Not Detected by Urinalysis	112a	21 USC 844	Yes
4F5	Manufacture Synthetic Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4F6	Wrongful Manufacture of Synthetic Drugs	112a	21 USC 841	Yes
4F7	Possession of Synthetic Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4F8	Wrongful Introduction of Synthetic Drugs	112a	21 USC 844	Yes
4F9	Introduction of Synthetic Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4G	Amphetamine/Methamphetamine/Barbiturates			
4G1	Wrongful Smuggling of Amphetamine/Methamphetamine/Barbiturates	112a	21 USC 844	Yes
4G2	Distribution of Amphetamine/Methamphetamine	112a	21 USC 841	Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
4G3	Wrongful Possession of Amphetamine/Methamphetamine	112a	21 USC 844	Yes
4G4A	Wrongful Use of Amphetamine/Methamphetamine Detected By Urinalysis	112a	21 USC 844	Yes
4G4B	Wrongful Use of Amphetamine/Methamphetamine Not Detected By Urinalysis	112a	21 USC 844	Yes
4G5	Manufacture Amphetamine/Methamphetamine W/Intent to Distribute	112a	21 USC 841	Yes
4G6	Wrongful Manufacture Amphetamine/Methamphetamine	112a	21 USC 841	Yes
4G7	Possession of Amphetamine/Methamphetamine W/Intent to Distribute	112a	21 USC 841	Yes
4G8	Wrongful Introduction of Amphetamine/Methamphetamine	112a	21 USC 844	Yes
4G9	Introduction of Amphetamine/Methamphetamine W/Intent to Distribute	112a	21 USC 841	Yes
4H	Prescription Drugs (Prescribed not Scheduled)(that is, oxycodine, ambien, etc.)			
4H1	Wrongful Smuggling of Prescription Drugs (Prescribed not Scheduled)	112a	21 USC 844	Yes
4H2	Distribution of Prescription Drugs(Prescribed not Scheduled)	112a	21 USC 841	Yes
4H3		112a	21 USC 844	Yes
4H4A		112a	21 USC 844	Yes
4H4B	Wrongful Use of Prescription Drugs Not Detected By Urinalysis(Prescribed not Scheduled)	112a	21 USC 844	Yes
4H7	Possession of Prescription Drugs W/Intent to Distribute (Prescribed not Scheduled)	112a	21 USC 841	Yes
4H8	Wrongful Introduction of Prescription Drugs (Prescribed not Scheduled)	112a	21 USC 844	Yes
4H9	Introduction of Prescription Drugs W/Intent to Distribute (Prescribed not Scheduled)	112a	21 USC 841	Yes
4J	Other drugs			
4J1	Wrongful Smuggling of Other Drugs	112a	21 USC 844	Yes
4J2	Distribution of Other Drugs	112a	21 USC 841	Yes
4J3	Wrongful Possession of Other Drugs	112a	21 USC 844	Yes
4J4A	Wrongful Use of Other Drugs Detected By Urinalysis	112a	21 USC 844	Yes
4J4B	Wrongful Use of Other Drugs Not Detected By Urinalysis	112a	21 USC 844	Yes
4J5	Wrongful Grow/Manufacture of Other Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4J6	Wrongful Grow/Manufacture of Other Drugs	112a	21 USC 841	Yes
4J7	Possession of Other Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4J8	Wrongful Introduction of Other Drugs	112a	21 USC 844	Yes
4J9	Introduction of Other Drugs W/Intent to Distribute	112a	21 USC 841	Yes
4M4B	Wrongful Use of an Inhalant (Article 92)	92		Yes*
4N4B	Wrongful Use of an Expired Prescription Drug (Article 92)	92		*Yes
4P4B	Wrongful Use of Synthetic Drugs (Not Scheduled) (Article 92)	92		*Yes
4X1	Conspiracy - Drug Offenses	81		*Yes
4X2	Solicitation to Commit Offense - Drug Offense	82		Yes
4X3	Accessory Before The Fact - Drug Offenses	77		*Yes
4X4	Accessory After The Fact - Drug Offenses	78		Yes

**Table C-1
Offense code list—Continued**

Offense code	Description	UCMJ Article	United States Code	CRC reportable
4X5	Obstruction of Justice - Drug Offenses	134		Yes
4X6	Misprision Serious Offense - Drug Offense	134		Yes
Persons Crime				
Offense Codes	Description	UCMJ Article	United States Code	CRC reportable
5B	Bigamy	134		Yes
5C1	Aggravated Assault	128	18 USC 1114	Yes
5C2	Assault	128	18 USC 114	Yes
5C5	Maiming	124		Yes
5D1	Child Neglect/Endangerment	134	18 USC 1169	Yes
5E	Civil Rights Violations	134	18 USC 242	Yes
5E6	Human Trafficking	Article 134 (Federal Assimilative Crimes Act)	18 USC 1546, 18 USC 1581, 18 USC 1584, 18 USC 1589, 18 USC 1590, 18 USC 1591, 18 USC 1592, 18 USC 1593, 18 USC 1594, 18 USC 1595, 18 USC 2423, 22 USC 7102	Yes
5F1	Extortion	127	18 USC 873	Yes
5G1	Forgery - Making/Altering/Uttering	123		
5H	Homicide	118		
5H1	Murder	118	18 USC 1111	Yes
5H2	Voluntary Manslaughter	119	18 USC 1112	Yes
5H3	Involuntary Manslaughter	119	18 USC 1112	Yes
5H3Q	Assault With Intent to Commit Manslaughter (Voluntary/Involuntary)	134	18 USC 1113	Yes
5H4	Negligent Homicide	134	18 USC 1112	Yes
5H5	Negligent Homicide - Traffic	134	18 USC 1112	Yes
5H6	Other Homicide (Justifiable)			Yes
5H7	Assault With Intent to Murder or attempted Murder	134	18 USC 1113	Yes
5H8	Accidental Death	No criminal act		Yes
5H9A	Death By Natural Causes	No criminal act		Yes
5H9B	Undetermined death	No criminal act		Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
5H9C1	Death by Hostile Forces			Yes
5H9C2	Death By Friendly Forces			Yes
5H9D	Sudden Unexplained Infant Death Syndrome (SUID) (formerly SIDS)			Yes
5J1	Impersonating Officer	134	18 USC 912	Yes
5J4	Unauthorized Wear of Military Uniform	134	18 USC 912	Yes
5K	Kidnapping	134	18 USC 1201	Yes
5K4	Missing Persons			Yes
5M1	Perjury (Give False Testimony)		18 USC 1621	Yes
5M2	False Swearing			Yes
5M3	False Official Statement		18 USC 1001	Yes
5M5	Subscribing False Statement		18 USC 621	Yes
5M6	Subornation of Perjury		18 USC 622	Yes
5M7	False Statement - Making/Signing	107	18 USC 1001	Yes
5N	Robbery	122	18 USC 1211	Yes
5N1	Assault With Intent to Rob	134		Yes
5P1	Attempted Suicide	No criminal act		Yes
5P2	Suicide	No criminal act		Yes
5T1	Communicating a Threat			Yes
5T3	Bomb Threat			Yes
5U1	Harassing Communications			Yes
5U3	Stalking			Yes
5X1	Conspiracy - Person Offenses			Yes
5X2	Solicitation to Commit Offense - Other Person Offense			Yes
5X3	Accessory Before The Fact - Person Offenses			Yes
5X4	Accessory After The Fact - Person Offenses			Yes
5X5	Obstruction of Justice - Person Offenses			Yes
5X6	Misprision Serious Offense	134		Yes
5Y2F	Dueling	114		Yes
5Y2H	Abusing Animal	134		No
5Y2N	Spying/Espionage	106	18 USC 792	Yes
5Y2P4	Aiding the Enemy	134	18 USC 792	Yes
5Y2P5	Harboring or Protecting Enemy	134	18 USC 792	Yes
5Y2P6	Giving Intelligence to Enemy	134	18 USC 792	Yes
5Y2P7	Communicating with Enemy	134	18 USC 792	Yes
5Y2P8	Misconduct as POW	134		Yes
5Y2Q	Looting, Pillaging	103		Yes
5Y3	Riot	116	18 USC 2101	Yes
5Y4	Breach of Peace	116		Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
5Y5	Provoking Speech/Gestures	117		Yes
5Z5	Terrorism - Planned	134	18 USC 2331 through 18 USC 2339	Yes
5Z6	Terrorism - Completed	134	18 USC 2331 through 18 USC 2239	Yes
Sex Crimes				
Offense Code	Description	UCMJ Article	United States Code	CRC reportable
6A	Child Molestation	120		Yes
6A1	Indecent Assault Upon a Child (FOR OFFENSES OCCURRING PRIOR TO 1 OCT 07)	134	18 USC 2251	Yes
6A2	Indecent Acts Upon A Child	120	18 USC 2251	Yes
6A3	Enticing A Child To Commit A Lewd Act	120	18 USC 2251	Yes
6A4	Exhibitionism or Lewd Gestures Toward a Minor(FOR OFFENSES OCCURRING PRIOR TO 1 OCT 07)	120	18 USC 2251	Yes
6A5	Aggravated Sexual Abuse of a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)	120		Yes
6A6	Indecent Liberty with a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)	120		Yes
6A7	Aggravated Sexual Contact with a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)	120		Yes
6A8	Abusive Sexual Contact with a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)	120		Yes
6A9	Sexual Abuse of a Child (FOR OFFENSES OCCURRING ON OR AFTER 28 Jun 12)	120b		Yes
6C1	Indecent Assault (Not Involving Sodomy) (FOR OFFENSES OCCURRING PRIOR TO 1 OCT 07)	120	18 USC 2242	Yes
6C5	Indecent Acts Between Adults & Minors (Not Involving Sodomy) (FOR OFFENSES PRIOR TO 1 OCT 07)	120	18 USC 2242	Yes
6C6	Wrongful Sexual Contact (From 1 Oct 07 through 27 Jun 12)	120		
6C7	Aggravated Sexual Contact (Adult)	120		
6C8	Abusive Sexual Contact (Adult)	120		
6C9	Indecent Acts (Adults) (From 1 Oct 07 through 27 Jun 12)	134		
6D1	Production/Publication Adult Pornography	134		No
6D2	Distribution of Adult Pornography	134		No
6D5	Possession of Adult Pornography w/intent to Distribute	134		No
6D7	Illegal Possession of Adult Pornography	120		No
6E1	Rape	120		Yes
6E2	Carnal Knowledge	120	18 USC 2243	Yes
6E3	Aggravated Sexual Assault	120		Yes
6E4	Sexual Assault	120 and 120b		Yes
6F	Forced Sodomy	125	18 USC 2241	Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
6G				Yes
6H1	Indecent Exposure (Other Sexual Misconduct)	120c		Yes
6J	Incest	120	18 USC 2243	Yes
6K1	Obscene Communication (via mail, telephone, digital, etc.)	134		Yes
6M	Voyeurism	134		*Yes
6M1	Indecent Viewing (Other Sexual Misconduct) (FOR OFFENSES OCCURRING ON OR AFTER 28 Jun 12)	120c		Yes
6M2	Indecent Visual Recording (Other Sexual Misconduct) (FOR OFFENSES OCCURRING ON OR AFTER 28 Jun 12)	120c		Yes
6M3	Indecent Broadcasting (Other Sexual Misconduct) (FOR OFFENSES OCCURRING ON OR AFTER 28 Jun 12)	120c		Yes
6N	Criminal Abortion	134		Yes
6P1	Adultery	134		Yes
6P2	Pandering	134		Yes
6P3	Prostitution	134	18 USC 1384	Yes
6Q1	Producing Child Pornography	134		Yes
6Q2	Distributing Child Pornography	134		
6Q3	Possessing Child Pornography With Intent to Distribute	134		
6Q4	Possessing, Receiving or Viewing Child Pornography	134		
6X1	Conspiracy - Sex Offenses	81		*Yes
6X2	Solicitation to Commit Sex Offenses	82	18 USC 373	Yes
6X3	Accessory Before The Fact - Sex Offenses	77	18 USC 2	*Yes
6X4	Accessory After The Fact - Sex Offenses	78	18 USC 3	*Yes
6X5	Obstruction of Justice -Sex Offenses	134	18 USC 1510	Yes
6Z	Sexual Assault Evidence Collection Kit	No criminal act		No
Property codes				
7A1	Aggravated Arson	126	18 USC 81	Yes
7A2	Simple Arson	126	18 USC 81	Yes
7B1	Black-market - Transfer/Possession	92		Yes
7B6	Unlawful Transfer/Possession of Items Through APO/FPO	92		Yes
7B7	Unlawful Currency Transactions	92		Yes
7B8	Organized Black-market Operations	92		Yes
7B9	Organized Currency Manipulation	92		Yes
7C1	Burglary	129	18 USC 2111	Yes
7C2	Housebreaking	130	18 USC 642	Yes
7C3	Unlawful Entry	134		Yes
7C4	Assault With Intent to Commit Burglary	134	18 USC 113	Yes
7C5	Assault With Intent to Housebreak	134	18 USC 642	Yes
7D1	Counterfeiting - Manufacture/Production	134	18 USC 471	Yes
7D2	Counterfeiting - Trafficking	134	18 USC 471	Yes
7D3	Counterfeiting - Passing	134	18 USC 471	Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
7D4	Counterfeiting - Possession	134	18 USC 471	Yes
7D5	Counterfeiting - Use	134	18 USC 472	Yes
7D6	False or Unauthorized Pass (making, altering, counterfeiting, or saling, etc.)	134	18 USC 545	Yes
7E	Smuggling	134	18 USC 641	Yes
7F1	Larceny of Govt Property	121		Yes
7F2	Larceny of Government Funds	121	18 USC 641	Yes
7F3	Wrongful Appropriation of Government Property	121	18 USC 2315	*Yes
7F4	Wrongful Disposition or Sale of Government Property	108	18 USC 641	Yes
7F5	Larceny of NAF Property	121	18 USC 641	Yes
7F6	Wrongful Appropriation of NAF property	121	18 USC 2315	*Yes
7F7	Wrongful Disposition or Sale of NAF Property	108	18 USC 641	Yes
7F8	Larceny of Govt Weapons/Munitions	121	18 USC 641	Yes
7F9	Larceny of Government Vehicle (motor/fixed wing/rotary, etc.)	121	18 USC 641	Yes
7G1	Larceny of Private Property	121	18 USC 641	Yes
7G2	Larceny of Private Funds	121	18 USC 641	Yes
7G3	Larceny of Private Vehicle (motor/boat/aircraft, etc.)	121		Yes
7G4	Making and Uttering Worthless Checks	134		Yes
7G5	Wrongful Appropriation of Private Property	121	18 USC 641	*Yes
7G6	Wrongful Appropriation of Private Vehicle (motor/boat/aircraft, etc.)	121		*Yes
7G7	Wrongful Disposition of Private Property	109	18 USC 2315	Yes
7H1	Larceny of/or From Mail		18 USC 1708	Yes
7H2	Obstructing or Secreting Mail		18 USC 1701	Yes
7H3	Destruction of Mail		18 USC 1703	Yes
7H4	Depositing Prohibited Matter in Mail		18 USC 1716e	Yes
7H5	Other Postal Violations		18 USC 1701	Yes
7H6	Mail Fraud		18 USC 1341	Yes
7H7	Destroy/Steal/Take/Open Mail	134	18 USC 1708	Yes
7H8	Depositing Obscenity in Mail	134	18 USC 1461	Yes
7H9	Other Mail Offenses	134	18 USC 1701	Yes
7J1	Wrongful destruction of Govt Property	108	18 USC 1361	Yes
7J2	Wrongful damage to Govt Property (Negligence/Willful)	108	18 USC 1361	Yes
7J3	Loss of Govt Property (Negligence/Willful)	108		Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
7J4	Wrongful Destruction of Private Property	109		Yes
7J5	Wrongful Damaging Private Property	109		Yes
7K1	Receiving Stolen Property	134	18 USC 662	Yes
7L	Failure to Pay Just Debt	134		Yes
7Q1	Waste or Spoil Captured Non-Military Property	109		Yes
7Q2	Fail to Secure Property	103		Yes
7Q3	Fail to Report/Turnover Property	103		Yes
7Q4	Dealing In Captured Property	103		Yes
7X1	Shoplifting	121	18 USC 641	Yes
7X2	Conspiracy - Property Offenses	81		*Yes
7X3	Solicitation to Commit Offense - Property Offenses	82	18 USC 373	Yes
7X4	Accessory Before The Fact - Property Offenses	77	18 USC 2	*Yes
7X5	Accessory After The Fact - Property Offenses	78	18 USC 3	*Yes
7X6	Obstruction of Justice - Property Offenses	134	18 USC 1510	Yes
Fraud crimes				
8A	Bribery/Graft	134	18 USC 201	Yes
8B	Conflict of Interest	134	18 USC 208	Yes
8B6	Confidential Information Disclosure (Trade Secrets Act)	134	18 USC 1905	Yes
8C	Dependency Assistance Fraud	134		Yes
8C3	False Claim	132	18 USC 287	Yes
8C4	Concealment, Removal or Mutilation of Records and Reports	132	18 USC 2071	Yes
8C5	Civil False Claims Act	132	31 USC 3729	Yes
8C6	False Bonds, Bids, and Public Records	132	18 USC 494	Yes
8C7	False Certification	132	18 USC 1018	Yes
8C8	Fraud and related activity in Connection with identification documents	132	18 USC 1028	Yes
8C9	Structuring Transaction to Evade Reporting Requirements	84	31 USC 5324	Yes
8D1	Effect Fraudulent Enlistment	84		Yes
8D2	Effect Fraudulent Separation	84		Yes
8D3	Effect Fraudulent Enlistment/Appointment	84		Yes
8D4	Fraudulent Assignment/Transfer	134		Yes
8D5	Fraudulent Personnel Action	132	18 USC 287	Yes
8E	Nonappropriated funds (fraud - make/present/using/claim - false document or signature)	132		Yes
8E8	Program Fraud Civil Remedies Act	132	31 USC 3801	Yes
8F	Pay and Allowance (Fraud - Make/Present/Using/Forgery/ False Document)	132		Yes
8G	Procurement/Salvage/Property Disposal Fraud	132		Yes
8H1	Fraud involving POL Items (not ration documents)	132		Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
8H2	Fraud involving POL Ration Documents	132		Yes
8H3	Fraud Pretaining to POL Items/POL Ration Documents involving Use of Computer	132		Yes
8J	Medical Treatment Fraud	132	18 USC 287	Yes
8K	Antitrust Violations	132		Yes
8L	Wire Fraud	132	18 USC 1343	Yes
8M	Procurement Fraud	132	18 USC 1031 18 USC 287	Yes
8M9	Major Fraud	132	18 USC 1031	Yes
8N1	Procurement Integrity Act-Disclosing/Obtaining Procurement Information	132	41 USC 2102 41 USC 2103 41 USC 2104	Yes
8N2	Fraud in Connection with Disaster or Emergency Benefits	132	18 USC 1040	Yes
8N3	Laundering of Monetary Instruments	132	18 USC 1956	Yes
8N4	Engaging in monetary transactions in property derived from specified unlawful activities	132	18 USC 1957	Yes
8P1	Computer Fraud - Obtaining Classified Information	134	18 USC 1030	Yes
8P2	Computer Fraud - Obtaining Financial/Credit Information	134	18 USC 1030	Yes
8P3	Computer Fraud - Unauthorized Access	134	18 USC 1030	Yes
8P4	Computer Fraud - Accessing With Intent to Defraud	134	18 USC 1030	Yes
8P5	Computer Fraud - Alter/Damage/Destroy Information	134	18 USC 1030	Yes
8P6	Computer Fraud - Alter/Damage/Destroy Medical Information	134	18 USC 1030	Yes
8P7	Computer Fraud - Trafficking Passwords and Other Access Codes	134	18 USC 1030	Yes
8Q	Restrictions on Post Government Employment	134	18 USC 203, 205, 207, 209, 208, 281 & 10 USC 2397 & 37 USC 801 & 41 USC 423	Yes
8R	Worker's Compensation Fraud	134	18 USC 1920	Yes
8S	Insufficient Fund Check - To Deceive/To Defraud	123a		
8T	Obtaining Services Under False Pretense	134		
8U	Burning With Intent To Defraud	134	18 USC 81	
8V1	Aircraft or Space Vehicle Parts Fraud	132	18 USC 38	Yes
8V2	Conversion of Property of Another	132	18 USC 654	Yes

Table C-1
Offense code list—Continued

Offense code	Description	UCMJ Article	United States Code	CRC reportable
8V3	Counterfeit Goods or Services-Trafficking	134	18 USC 2320	Yes
8V4	Defective National Defense Material	132	18 USC 2156	Yes
8V5	Defective War Material	132	18 USC 2154	Yes
8V6	Illegal Gratuities	134	18 USC 201c	Yes
8V7	Bid Rigging/Sherman Anti-Trust Act	132	15 USC 1, 2, 3	Yes
8V9	Kickbacks (Prohibited Acts)	134	41 USC 8702, 8706, 8707	Yes
8W	Violation of Safe Drinking Water Act	134	42 USC 300	Yes
8W1	Clean Air Act	134	31 USC 3729	
8W2	Clean Water Act	134	33 USC 1319 (c) (1) & (2)	Yes
8W3	Resource Conservation and Recovery Act	134	42 USC 6928(d)(2)(A)	Yes
8W4	Comprehensive Environmental Response, Compensation, and Liability Act	134	42 USC 9603(b)	Yes
8W5	Hazardous Materials Transportation Act	134	49 USC 103, 104, and 106	Yes
8W6	Toxic Substances Control Act	134	15 USC 2601	Yes
8W7	Violation of OSHA Asbestos Act	134	29 USC 655 & 40 USC 333	Yes
8W8	Violation of National Environmental Protection Act	134	42 USC 4321-4370a	Yes
8W9	Violation of Medical Waste Tracking	134	42 USC 6901	Yes
8X1	Other Fraud Offense Involving Use of a Computer	134		Yes
8X2	Conspiracy - Fraud Offenses	81	18 USC 1028	*Yes
8X3	Solicitation to Commit Offense - Fraud Offenses	82	18 USC 373	Yes
8X4	Accessory Before The Fact - Fraud Offenses	77	18 USC 2	*Yes
8X5	Accessory After The Fact - Fraud Offenses	78	18 USC 3	*Yes
8X6	Obstruction of Justice - Fraud Offenses	134	18 USC 1510	Yes
8Y	Government Credit Card Fraud	132		Yes
8Y1	Government Purchase Card Fraud	132	18 USC 287	Yes
8Y2	Government Travel Card Fraud	132	18 USC 287	Yes
8Y3	Other Government Card Fraud	132		Yes
8Y4	Government Fuel Card Fraud	132		Yes
8Z1	RICO (Criminal)	134	18 USC 1963	Yes
8Z2	RICO (Civil)	134	18 USC 1964	Yes

Table C-2
Offense codes for Army investigation reports

Offense code	Special investigative code descriptions	CRC reportable
9A1	Crime analysis (Crime trend at an installation)	No
9A1A	Crime analysis - Crimes against persons	No
9A1B	Crime analysis - Crimes against property	No
9A1C	Crime analysis - General (combination of categories)	No
9A1D	Crime Analysis - Other	No
9A1E	Drug assessments	No
9A2	CPS - Logistical (DPDO, ammunition plants, and so forth)	No
9A3	CPS - Installation support activities (clubs and so forth)	No
9A4	Personnel security vulnerability assessments	No
9B	Improper police profiling/bias (allegations/violations)	No
9C	Civil litigation	No
9D1	Narcotics/contraband detector dog	No
9D1A	Drug detection dogs - marijuana/hashish	No
9D2	Explosive detector dog	No
9D3	Patrol dog	No
9E	Physical security survey	No
9F	Protective services	No
9G1	Polygraph examination	No
9G2	Crime laboratory analysis	No
9G2A	Chemistry	No
9G2B	Latent prints	No
9G2C	Firearms/tool marks	No
9G2D	Forensic documents	No
9G2E	Digital evidence (USACIL and so forth)	No
9G2F	Other	No
9G2G	Trace evidence	No
9G2H	Serology/DNA	No
9G2J	CODIS	No
9G3	Investigative hypnosis	No
9G4	Digital evidence	No
9G5	Cyber-related incident (Internet/online)	No
9H	Criminal information	No
9J	War crimes	No
9K	Voluntary disclosure investigations	No

Table C-2
Offense codes for Army investigation reports—Continued

9L	Qui Tam investigation	No
9M	Top 100 defense contractor investigations	No
9M1	Procurement: Contract awarded to a top 100 contractor	No
9M2	Contract awarded to a subsidiary of a top 100 contractor	No
9M3	Contract involving contingency operations	No
9N1	Protective order issued - military	No
9N2	Protective order issued - civilian	No
9Q	Registration of convicted sex offender	No
9R	Reverse drug operation	No
9S	Gang involvement	No
9T	One station unit training	No
9T1	Advanced individual training	No
9T2	Professional development training	No
9T3	Basic training	No
9U1	Family abuse (domestic) - adult	No
9U2	Family abuse (domestic) - child	No
9V1	Direct threat to CID principal/protectee	No
9V2	Indirect/veiled threat to CID principal/protectee	No
9V3	Inappropriate communications to CID principal/protectee	No
9W	Electronic surveillance (TLE, pre-test, and so forth)	No
9X	Hazing/bullying or suspected hazing/bullying incident	No
9Y	Return to military control (RMC)	No
9Z	Suspicious activity reporting (SAR)	No
9Z1	SAR Department of Defense categories	No
9Z1J	Sabotage, tampering, and/or vandalism	No
9Z1K	Surveillance	No
9Z1M	Theft, loss, and/or diversion	No
9Z1N	Weapons discovery	No

*More information required to equate to a CRC reportable offense CRC Reportable Offenses: punishment of 6 months or more; known subject; founded

Appendix D Internal Control Evaluation

D-1. Functions

The functions covered by this checklist are the administration of the Law Enforcement Reporting System, use of the U.S. District Court Central Violations Bureau Form, the SIR procedures, the SAR system, and use of the NCIC.

D-2. Purpose

The purpose of this checklist is to help assessable unit managers and management control administrators evaluate the key management controls outlined below. It is not intended to cover all controls.

D-3. Instructions

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years.

D-4. Test questions

- a. Are law enforcement and PMO administrative personnel trained in the use of ALERTS, which is DA Form 190-45-SG?
- b. Are procedures in place to ensure that release of law enforcement information is done in accordance with the FOIA, The Privacy Act, and this regulation?
- c. Are procedures in place to ensure that police intelligence information is purged as required by this regulation?
- d. Does the system administrator for ALERTS, the DA Form 190-45-SG, maintain control and accountability of personnel using the system?
- e. Are procedures in place to ensure that reports of a commander's action taken are returned to the PMO in a timely manner?
- f. Are both military and civilian protection orders being entered into ALERTS, the DA Form 190-45-SG?
- g. Are PMs or DESs reporting incidents that occur off the installation in their geographic areas, in accordance with table 1-1 of AR 190-45?
- h. Are thefts, suspected thefts, wrongful appropriation, or willful destruction of Government property or appropriated funds valued at more than \$100,000 being reported as a category-2 SIR?
- i. Are category-1 serious incidents being reported to HQDA within 12 hours of discovery or notification at the installation level?
- j. Are "add-on" SIRs being completed to provide information not available at the time of the original report?
- k. Are category-2 serious incidents being reported to HQDA within 24 hours of discovery or notification at the installation level?
- l. Are law enforcement personnel issuing a separate U.S. District Court Violations Notice (Central Violations Bureau Form) for each offense or violation?
- m. Are procedures in place to ensure that each Central Violations Bureau Form is accounted for?
- n. Are procedures in place to ensure that each Central Violations Bureau Form is completed properly, in accordance with CVB procedures?
- o. Are procedures in place to ensure that all violations issued on the Central Violations Bureau Form are entered into DA Form 190-45-SG?
- p. Are procedures in place to ensure that the release of law enforcement information is being handled in accordance with the FOIA, The Privacy Act, and chapter 3 of this regulation?
- q. Are installation PMs or DESs appointing NCIC terminal coordinators?
- r. Are terminal coordinators ensuring that NCIC use is limited to authorized criminal justice purposes?
- s. Are only trained personnel allowed to operate NCIC terminals?
- t. Are requests for NCIC participation initiated by the PM or DES and submitted to the garrison commander?
- u. Are notifications of serious violation, suspension, or revocation from the use of NCIC and State government terminals and NCIC files immediately reported to the Director, USACRC's Federal service coordinator by the most expeditious means?
- v. Are all Government or privately owned weapons reported lost, stolen, or recovered entered into the NCIC gun file, regardless of value?
- w. Have PM or Directorate of Emergency Services personnel whose law enforcement responsibilities require access to the eGuardian system applied directly to the FBI for access via the Law Enforcement Online Web site?
- x. Has implementation and establishment of user account protocols and account management procedures, to include obtaining FBI user training prerequisites and account deactivation protocols placed in action?

- y. Are procedures in place to ensure that release of SAR information is done in accordance with FOIA, The Privacy Act, and this regulation?
- z. Does the program manager for eGuardian maintain control and accountability of personnel using the system?
 - aa. Are unknown subject thefts or suspected thefts, wrongful appropriation, or willful destruction of Government property or appropriated funds valued at more than \$100,000 being reported as an SAR?
 - ab. Are specific-and-actionable SARs being reported to HQDA within 24 hours of discovery or notification at the installation level?
 - ac. Are procedures in place to ensure that non-actionable SAR reporting is made within 72 hours?
 - ad. Did the installation PM or DES appoint a SAR coordinator?
 - ae. Are only trained LE personnel obtaining eGuardian accounts?
 - af. Are notifications of serious violations, suspension, or revocation from the use of eGuardian immediately reported to the FBI by the most expeditious means?
 - ag. Are SARs initiated on all Government or privately owned weapons that are reported lost, stolen, or recovered regardless of value?
 - ah. Has the eGuardian program manager provided adequate guidelines and oversight to define properly its use and to ensure adequate protections, including 6 USC 1104 (Immunity for reports of suspected terrorist activity or suspicious behavior and response), relating to SARs?
 - ai. Do the eGuardian reports comply with the standards outlined in the applicable regulations?
 - aj. Are reports retained in the eGuardian SDR programmed for retention for a period of 5 years?
 - ak. Are SARs that are entered into the eGuardian SDR, and resolved as having no clear link to terrorism as a result of an FBI Joint terrorism task force or DCIO investigation, removed from the eGuardian system after 180 days?
 - al. Is the installation PM or DES in compliance with 5 USC 552A (The Privacy Act), implemented in the DOD by DODD 5400.11 and DOD 5400.11–R, other Federal laws, and DOD regulations in the collection, use, storage, and dissemination of personally identifiable information concerning U.S. persons?

D–5. Supersession

No previous management control evaluation checklist exists for this program.

D–6. Comments

Help to make this a better tool for evaluating management controls. Submit comments to: HQDA, PMG (DAPM–MPO–LE), 2800 Army Pentagon, Washington, DC 20318–2800.

Glossary

Section I Abbreviations

AA&E

arms, ammunition, and explosives

AARA

access and amendment authority

ACOM

Army command

AFI

Air Force instruction

AKO

Army Knowledge Online

ALERTS

Army Law Enforcement Reporting and Tracking System (DA Form 190–45–SG)

AMC

Army Materiel Command

APD

Army Publishing Directorate

APO

Army Post Office

AR

Army regulation

ARNG

Army National Guard

ARNGUS

Army National Guard of the United States

ASA

Army Support Activity

ASAP

Army Substance Abuse Program

ASCC

Army service component command

AWOL

absence without leave

BSAT

biological select agents and toxins

CAC

common access card

CD

compact disc

CDR

commander

CFR

Code of Federal Regulations

CG

commanding general

CI

counterintelligence

CICR-FP**CID**

criminal investigation division

CIOC

Command Intelligence Operation Center

CJCS

Chairman of the Joint Chiefs of Staff

CJCSM

Chairman of the Joint Chiefs of Staff manual

CJIS

Criminal Justice Information System

CONUS

continental United States

CPO

civilian protection order

CRC

Crime Records Center

CRIMINTEL

criminal intelligence

CTA

control terminal agency

CVB

Central Violations Bureau

DA

Department of the Army

DAMI-CD**DA PAM**

Department of the Army pamphlet

DCII

defense central investigations index

DD

Department of Defense form

DES

Director of Emergency Services

DIBRS

Defense Incident-Based Reporting System

DLAR

Defense Logistics Agency Regulation

DMV

Department of Motor Vehicles

DNA

deoxyribonucleic acid

DOB

date of birth

DOD

Department of Defense

DODD

Department of Defense directive

DODI

Department of Defense instruction

DODM

Department of Defense manual

DOJ

Department of Justice

DRU

direct reporting unit

DSN

defense switched network

DTM

Directive-Type Memorandum

EO

Executive Order

FM

field manual

FBI

Federal Bureau of Investigation

FOIA

Freedom of Information Act

FOUO

for official use only

HQDA

Headquarters, Department of the Army

IAFIS

Integrated Automated Fingerprint Identification System

IMCOM

Installation Management Command

LE

law enforcement

LER

Law Enforcement Report

LSD

lysergic acid diethylamide

MCO

Marine Corps order

MEDCOM

Medical Command

MOU

memorandum of understanding

MP

military police

MPC

military police code

MPRS

Military Police Reporting System

MRRP

Military Police Reporting Program Records

MST

material support to terrorism

MTF

medical treatment facility

NAF

non appropriated fund

NCIC

National Crime Information Center

NIBRS

National Incident Based Reporting System

NICS

National Instant Checks System

NLETS

National Law Enforcement Telecommunications Systems

NMN

no middle name

NTA

notice to appear

OCONUS

outside continental United States

OPMG

Office of the Provost Marshal General

OPREP-3

operational reporting-3

OPREP-3P

operational reporting-3 pinnacle

ORI

originating agency identifier

OSD

Office of the Secretary of Defense

PAO

public affairs officer

PAS

Privacy Act Statement

PCP

phencyclidine

PI

protected identity

PII

Personally identifiable information

PL

Public Law

PM

provost marshal

PMG

Provost Marshal General

PMO

provost marshal office

POB

place of birth

POW

prisoner of war

PPE

personal protective equipment

RCM

rule for court-martial

RMC

returned to military control

SAR

suspicious activity report

SARC

sexual assault response coordinator

SCA

special category absentee

SDDC

Surface Deployment and Distribution Command

SIR

serious-incident report

SJA

Staff Judge Advocate

SOP

standard operating procedures

SORN

System of Records Notice

SSN

social security number

TRADOC

Training and Doctrine Command

UCMJ

Uniform Code of Military Justice

UCR

uniform crime report

UIC

unit identification code

USACIDC

U.S. Army Criminal Investigation Command

USACIL

U.S. Army Criminal Information Laboratory

USACRC

U.S. Army Crime Records Center

USADIP

U.S. Army Deserter Information Point

USAG

U.S. Army Garrison

USAR

U.S. Army Reserve

USARC

U.S. Army Reserve Command

USAREUR

U.S. Army Europe

USARPAC

U.S. Army Pacific

USC

United States Code

USSS

United States Secret Service

VCIS

Voice Case Information System

VCR

videocassette recorder

VRS

Vehicle Registration System

Section II**Terms****Adult offender**

A criminal offender who has attained the age of 18, or who, although under the age of 18, was a member of the military at the time of the offense. This includes emancipated minors and those minors who are married. This will also include juveniles who are prosecuted as adult offenders.

Anti-bias

A crime against an individual or organization based upon race, ethnic background, religious or sexual orientation. (See also hate crime).

Army interest

Incidents or offenses of interest to the Army because Army personnel are involved, the Army is a victim of the offense, or other substantive ties to the Army or DOD exist.

Barred or expelled person

A person against whom administrative action has been imposed by the installation commander to preclude future entry or continued presence on the installation.

Blotter extract

A single or series of entries removed from the chronological form of the full MP blotter, and reflecting the relevant information required by the specific recipient of the extract.

Bomb threats

Communication by any means specifically threatening to use a bomb to attack against U.S. forces, facilities, or missions.

Category 1 serious incident

A serious incident that is of immediate concern to HQDA. Incidents that must be reported to HQDA as Category 1 serious incidents are listed in chapter 8, paragraph 8-2.

Category 2 serious incident

A serious incident that is of concern to HQDA. Incidents that must be reported to HQDA as Category 2 serious incidents are listed in chapter 8, paragraph 8-3.

Category 3 serious incident

An incident that is of concern to the IMCOM region, ACOM, ASCC, or DRU (see chapter 8 paragraph 8–4), any incident that must be reported to the IMCOM region, ACOM, ASCC, or DRU as a category 3 serious incident according to an approved IMCOM region, ACOM, ASCC, or DRU supplement to this regulation. Establishment of category 3 serious incidents is neither required nor reportable to HQDA.

Collateral

A fixed sum which is paid in lieu of appearance in court.

Control Terminal Agency

A state criminal justice agency on the NCIC System providing statewide service to criminal justice users with respect to NCIC data.

Controlled cryptographic items

Controlled cryptographic items are described as secure telecommunications or information handling equipment, associated cryptographic components, or other hardware items, which perform a critical communication security function.

Controlled inventory item code

Controlled inventory item codes are items that require quarterly inventory with characteristics that require special identification accounting, security, or handling to ensure their safeguard. These items are considered controlled items that require a high degree of protection and control, because of statutory requirements, or regulations; high-value, highly technical, or hazardous items; small arms, ammunition, explosives, demolition material, night vision devices, and navigation systems.

Criminal history file

Information collected by criminal justice agencies on individuals consisting of descriptions of an individual, notations of arrest, detentions, indictments on serious criminal charges, and any disposition. The term does not include identification information such as fingerprints.

Criminal investigation

An investigation of a criminal incident, offense, or allegation conducted by law enforcement personnel

Criminal justice

Pertaining to the enforcement of criminal laws, including efforts to prevent, control, or reduce crime, or to identify, apprehend, and prosecute criminal offenders.

Criminal offense

Any act or omission defined and prohibited as a criminal act by the UCMJ, the USC, state and local codes, foreign law, or international law or treaty. For juveniles, this term refers to acts which, if committed by an adult, would be subject to criminal penalties.

Dangerous drugs

Non-narcotic drugs that are habit forming or have a potential for abuse because of their stimulant, depressant, or hallucinogenic effect, as determined by the Secretary of Health and Human Services or the Attorney General of the United States. A dangerous drug is a drug that is not safe for self-medication and is not included in Schedules I–V.

Disclosure

The furnishing of information about an individual, by any means, to an organization, Government agency, or to an individual who is not the subject of the record, the subject's designated agent, or legal guardian.

Elicitation

Any attempts to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and the need-to-know. Elicitation attempts will be made by mail, fax, telephone, by computer, or in person.

Evidence kit

A sexual assault evidence-collection kit.

Family member

Includes those individuals for whom the Service member provides medical, financial, and logistical (for example,

housing, food, and clothing) support. This includes, but is not limited to, the spouse, unmarried dependent child under 22 years of age, including an adopted child or natural child, elderly adults, and persons with disabilities.

Founded offense

An offense adequately substantiated by police investigation as a violation of the UCMJ, the USC, state and local codes, foreign law, international law or treaty, regulation, or other competent policy. Determination that an offense is founded is a law enforcement decision based on probable cause supported by corroborating evidence and is not dependent on final adjudication.

Gang

A group of individuals whose acts of crime are committed against the public at large as well as other groups. A gang usually has in common one or more of the following traits: geographic area of residence, race, or ethnic background. They have a defined hierarchy that controls the general activities of its members.

Hate crime

Crimes directed against persons, places of worship, organizations (and their establishments where individuals gather), because of their race, ethnic background, religious, or sexual orientation.

Indexed

Refers to the procedure whereby an organization responsible for conducting criminal investigations submits identifying information concerning subjects, victims, or incidentals of investigations for addition to the Defense Clearance and Investigations Index (DCII).

Informant

A person who agrees to confidentially collect or provide recurring information of law enforcement value to police agencies.

Initiating Provost Marshal/Director of Emergency Services

The PM/DES who first records a complaint, initiates police actions, and subsequently initiates an LER on a criminal offense or incident.

Investigative jurisdiction

Jurisdiction with responsibility to investigate criminal offenses based on geographical boundaries or the category of the offense.

Juvenile

A subject of an incident who is under the age of 18, who was not a military member, spouse of a military member, or otherwise having been declared to have reached their majority at the time of an offense.

Law enforcement activity

An activity engaged in the enforcement of criminal laws to prevent, control and reduce crime, and apprehend criminals.

Live scan

An electronic finger and/or palm print capturing system.

Military offense

Any offense unique to the military. Examples are AWOL, desertion, and uniform violations.

Military police

Any type of DOD, Army, contracted, or contractor police or security forces responsible for performing law enforcement or security on Army installations.

Misdemeanor

Any offense not punishable by death or imprisonment for a term exceeding 1 year. Included are violations of those provisions of state laws made applicable to military reservations by 18 USC 13 (The Assimilated Crimes Act).

Multiple offenses

Two or more offenses occurring within the same reported incident (for example, murder, rape, and robbery of a single victim).

Non-specific threats

Threats received by any means, which contain a specific time, location, or area for an attack against U.S. forces, facilities, or missions. This includes, but is not limited to, any event or incident, or series of events or incidents, which in and of themselves will indicate the potential for a threat to U.S. forces, facilities, or mission, regardless of whether the threat posed is deliberately targeted or collateral.

Name check

Procedure to determine the existence of prior civilian or military criminal records on an individual.

National Crime Information Center

A nationwide computerized information System established as a service to all criminal justice agencies.

National Law Enforcement Telecommunications Systems

Computer-controlled message switching network linking local, state, and Federal criminal justice agencies together for the purpose of information exchange.

Offender (same as subject)

Person identified and reported by law enforcement officials as the person who committed an offense. Determination that a person committed an offense is based on probable cause supported by corroborating evidence.

Offender disposition

The result of actions taken by commanders, supervisors, and military or civil courts to dispose of founded offenses. These actions will be judicial, non-judicial, or administrative.

Officer

Any Army installation law enforcement agent, either military or civilian, who is authorized to issue U.S. District Court Central Violations Bureau Form (including Statement of Probable Cause and, if appropriate, Promise to Appear portions of the U.S. District Court Central Violations Bureau Form).

Originating agency identifier

An identifier assigned by the FBI to an agency meeting the criteria for participation in the NCIC.

Originating law enforcement agency

Military or civilian law enforcement activity where a criminal incident was originally reported or investigated.

Personal information

Information about an individual that is intimate or private to the individual, as distinguished from information concerning the person's official functions or public life.

Petty offense

Minor misdemeanors that are not punishable by imprisonment for more than 6 months or a fine of more than \$500.

Pledge of confidentiality

Promise not to disclose to an unauthorized person or agency information provided by an individual in confidence.

Police intelligence

Information compiled in an effort to anticipate, prevent, or monitor possible or potential criminal activity directed at or affecting the Army, or Army personnel.

Protected identity

A term used in preparation of RDFs and Serious Incident Reports to replace the name and personal data of juvenile subjects and certain other individuals. This term may also be used for juvenile victims in sensitive cases such as child abuse, incest or rape.

Provost Marshal/Director of Emergency Services

The senior officer, military or civilian directly responsible for law enforcement and security, regardless of the individual's position or title (for example, security officer, security director, and security manager). This individual must occupy a position that involves the administration of criminal justice.

Records custodian

Person charged with responsibility for proper processing, storage, safekeeping, and disposition of records containing personal information relevant to criminal investigations.

Redacted

Editing PI from military police reports to send to outside agencies.

Repetitive activities

Any activities that meet one of the other criteria listed in chapters 2 through 5 and have occurred two or more times or the same activity by the same person and/or vehicle, within a one month period.

Restricted entry

A term used in preparation of an RDF, to replace a blotter entry for which dissemination of any information concerning the incident is controlled or restricted.

Serious domestic violence

Any incident of domestic violence where a weapon (such as a firearm, knife or motor vehicle) is involved; the victim suffers a broken limb, is injured during pregnancy, is sexually abused, is choked or strangled or is admitted to the hospital because of injuries incurred during the incident; domestic violence incidents where a violation of a protective order (military or civilian) has occurred.

Serious incident

Any actual or alleged incident, accident, misconduct, or act, primarily criminal in nature, that, because of its nature, gravity, potential for adverse publicity, or potential consequences warrants timely notice to HQDA.

Serious incident report

A formal notification to HQDA of a serious incident as prescribed by this regulation.

Special Latent Cognizant File

A manually concentrated subset of the Criminal Master File that consists of 35 separate files with a total capacity of 1.5 million subjects, such as terrorists, disaster victims, serial crimes, and so forth).

Subject (same as offender)

Person identified and reported by law enforcement officials as the person who committed an offense. Determination that a person committed an offense is based on probable cause supported by corroborating evidence.

Surveillance

Any reported possible activity in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts will include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or other vision-enhancing devices, or any reports from host nation security forces of possible surveillance of U.S. assets.

Suspicious activities/incidents

Any activity/incident that does not specifically fit into one of the other six categories in paragraph 2–5 yet is believed to represent a force protection threat.

Temporary custodian

An individual or organization other than the originating MP organization in possession of, or with access to MP files or records.

Tests of security

Any attempts to measure security reaction times or strengths; any attempts to test or to penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, passes, or other security related documents.

Titled

Placing the name(s) of a person, corporation(s), or other legal entity, organization(s), or other occurrence(s) in the subject block of a criminal investigative report.

Unfounded offense

A criminal complaint in which a determination is made that a criminal offense was not committed or did not occur.

This determination is based on police investigation and not on court-martial findings, civil court verdicts, or command determinations.

User agreement

A document describing operating policies and responsibilities between an installation PM/DES and a State CTA.

Victim

A person who has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime committed in violation of the UCMJ, or in violation of the law of another jurisdiction if any portion of the investigation is conducted primarily by the DOD components. Such individuals will include, but are not limited to, the following: (1) Military members and their Family members. (2) When stationed outside the continental United States, DOD civilian employees and contractors, and their Family members, in stateside locations, such as medical care in military medical facilities. (3) When a victim is under 18 years of age, incompetent, incapacitated or deceased, the term includes one of the following (in order of preference): a spouse; legal guardian; parent; child; sibling; another Family member; or another person designated by a court or the component responsible official, or designee. (4) For a victim that is an institutional entity, an authorized representative of the entity. Federal Departments and State and local agencies, as entities, are not eligible for services available to individual victims.

Witness

A person who has information or evidence about a crime and provides that knowledge to a DOD component concerning an offense within the component's investigative jurisdiction. When the witness is a minor, this term includes a Family member or legal guardian. The term "witness" does not include a defense witness or any individual involved in the crime as a perpetrator or accomplice.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 002222-000