PART 635—LAW ENFORCEMENT REPORTING

Subpart A—Records Administration

Subpart B—Release of Information

Subpart C—Offense Reporting

Subpart D—Victim and Witness Assistance Procedures

Subpart E—National Crime Information Center Policy

AUTHORITY: 28 U.S.C. 534, 42 U.S.C. 10601, 18 U.S.C. 922, 10 U.S.C. 1562, 10 U.S.C. Chap. 47, 42 U.S.C. 16901 *et seq.*, 10 U.S.C. 1565, 42 U.S.C. 14135a.

SOURCE: 80 FR 28549, May 19, 2015, unless otherwise noted.

Subpart A—Records Administration

§ 635.1 General.

The proponent of this part is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this Part that are consistent with controlling law and regulations. In distributing information on juvenile victims or subjects, the installation Freedom of Information Act (FOIA) Office will ensure that only individuals with a need to know of the personally identifiable information (PII) of a juvenile are provided the identifying information on the juvenile. For example, a community commander is authorized to receive pertinent information on juveniles under their jurisdiction. When a Law Enforcement Report identifying juvenile offenders must be provided to multiple commanders or supervisors, the FOIA Office must sanitize each report to withhold juvenile information not pertaining to that commander's area of responsibility.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.2 Safeguarding official information.

(a) Military police records are unclassified except when they contain national security information as defined in AR 380–5 (Available at *http://www.apd.army.mil/pdffiles/r380_5.pdf*), Department of the Army Information Security Program.

(b) Military police records will also be released to Federal, state, local or foreign law enforcement agencies as prescribed by 32 CFR part 505, The Army Privacy Program. Expanded markings will be applied to these records.

§ 635.3 Special requirements of the Privacy Act of 1974.

(a) Certain PII is protected in accordance with the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, as implemented by 32 CFR part 310, DoD Privacy Program, 32 CFR part 505, The Army Privacy Program, and OMB guidance defining PII.

(b) Pursuant to 5 U.S.C. 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 (PAS). A PAS 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 law enforcement personnel performing official duties often require an individual's PII, including SSN, for identification purposes. This PII can be used to complete law enforcement reports and records. In addition to Executive Order 9397, as amended by Executive Order 13478, the solicitation of the SSN is authorized by paragraph 2.c.(2) of DoD Instruction 1000.30, ''Reduction of Social Security Number (SSN) Use Within DoD'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/100030p.pdf*). 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/alternate means of identification to facilitate filing and retrieval. The following procedures will be used for identification:

(1) Retired military personnel are required to produce their Common Access Card or DD Form 2 (Ret) (U.S. Armed Forces of the United States General Convention Identification 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 law enforcement reports and related forms.

(3) Non-Department of Defense (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) 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, The Army Privacy Program, *http://www.apd.army.mil/pdffiles/r340_21.pdf*, provides that records contained in SORN A0190–45, Military Police Reporting Program Records (MRRP), *http://dpcld.defense.gov/Privacy/SORNsIndex/tabid/5915/Article/6066/a0190-45-opmg.aspx*, 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.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.4 Police intelligence/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. 32 CFR part 633 designates the U.S. Army Criminal Investigation Command (USACIDC) as having the primary responsibility to operate a criminal intelligence program. Criminal Intelligence will be reported through the Army Criminal Investigation and Criminal Intelligence (ACI2) System and other criminal intelligence products. The crimes listed in paragraphs (a)(1)–(9) of this section, as well as the reportable incidents, behavioral threat indicators, and other matters of counterintelligence interest specified by AR 381–12, Threat Awareness and Reporting Program, (available at *http://www.apd.army.mil/pdffiles/r381_12.pdf*) will be reported to the nearest Army counterintelligence 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 info.

(b) Information on persons and organizations not affiliated with DoD may 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 law enforcement agencies which directly pertains to the law enforcement mission and activity of the installation Provost Marshal Office/Directorate of Emergency Services (PMO/DES), Army Command (ACOM), Army Service Component Command (ASCC) or Direct Reporting Unit (DRU) PMO/DES, or that has a clearly identifiable military purpose and connection. A determination that specific information may 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 part. The policies in this section 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 DoD Directive 5200.27 (available at *http://www.dtic.mil/whs/directives/corres/pdf/*520027p.pd), AR 380–13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations (available at *http://www.apd.army.mil/pdffiles/r380__13.pdf*) and AR 25–400–2, The Army Records Information Management System (ARIMS) (available at *http://www.apd.army.mil/pdffiles/r25__400__2.pdf*).

(d) Local police intelligence files may be exempt from 32 CFR part 518 and the FOIA's disclosure requirements.

§ 635.5 Name checks.

(a) Information contained in military police records will be released under the provisions of 32 CFR part 505, The Army Privacy Program, to authorized personnel for valid background check purposes. Examples include child care/youth program providers, sexual assault response coordinator, unit victim advocate, access control, unique or special duty assignments, security clearance procedures and suitability and credentialing purposes. Any information released must be restricted to that necessary and relevant to the requester's official purpose. Provost Marshals/Directors of Emergency Services (PM/DES) will establish written procedures to ensure that release is accomplished in accordance with 32 CFR part 505.

(b) Checks will be accomplished by a review of the Army's Law Enforcement Reporting and Tracking System (ALERTS). Information will be disseminated according to subpart B of this part.

(c) In response to a request for local files or name checks, PM/DES will release only founded offenses with final disposition. Offenses determined to be unfounded will not be released. These limitations do not apply to requests submitted by law enforcement agencies for law enforcement purposes, and counterintelligence investigative agencies for counterintelligence purposes.

(d) A successful query of ALERTS would return the following information:

(1) Military Police Report Number;

(2) Report Date;

(3) Social Security Number;

(4) Last Name;

(5) First Name;

(6) Protected Identity (Y/N);

(7) A link to view the military police report; and

(8) Whether the individual is a subject, victim, or a person related to the report disposition.

(e) Name checks will include the information derived from ALERTS and the United States Army Crime Records Center (USACRC). All of the policies and procedures for such checks will conform to the provisions of this part. Any exceptions to this policy must be coordinated with Headquarters Department of the Army (HQDA), Office of the Provost Marshal General (OPMG) before any name checks are conducted. The following are examples of appropriate uses of the name check feature of ALERTS:

(1) Individuals named as the subjects of serious incident reports.

(2) Individuals named as subjects of investigations who must be reported to the USACRC.

(3) Individuals seeking employment as child care/youth program providers.

(4) Local checks of the ALERTS as part of placing an individual in the ALERTS.

(5) Name checks for individuals seeking employment in law enforcement positions.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.6 Registration of sex offenders on Army installations (inside and outside the Continental United States).

(a) *Sex Offenders on US Army Installations.* Garrison Commander's responsibilities: Garrison Commanders will ensure that sex offenders, as defined in paragraph (b) of this section that reside or are employed on an Army Installation register with the installation PM/DES. This includes service members, civilian employees, accompanying dependent family members, and contractors subject to the incorporation of the sex offender registration requirement into the contract.

(b) 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 United States 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, Military Justice (available at *http://www.apd.army.mil/pdffiles/r27_10.pdf*), Chapter 24.'' See 42 U.S.C. 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 Offender Registration Requirements. Sex offenders, as defined in paragraph (b)(1) of this section must register with the installation PMO/DES within three working days of first arriving on an installation. Sex offenders must provide the installation PMO/DES with evidence of the qualifying conviction. The PMO/DES will enter the registering sex offender's conviction information on a Raw Data File as an information entry into the Army's Law Enforcement Reporting and Tracking System (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/DES does not relieve sex offenders of their legal obligation to comply with applicable state and local registration requirements for the state in which they reside, work, or attend school (see, AR 190–47 (available at *http://www.apd.army.mil/pdffiles/r190_47.pdf*), chapter 14 and AR 27–10 (available at *http://www.apd.army.mil/pdffiles/r27_10.pdf*), chapter 24). Registration with the state is also required under the Sex Offender Registration and Notification Act (SORNA), 42 U.S.C. 16901 *et seq.*, and implemented by AR 27–10 (Available at *http://www.apd.army.mil/pdffiles/r27_10.pdf*), Military Justice, and DoDI 1325.7 (Available at *http://www.dtic.mil/whs/directives/corres/pdf/132507p.pdf*). In addition, upon assignment, reassignment, or change of address, sex offenders will inform the installation PM/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)(1) of this section in which a sex offender is required to register.

(d) Installation PMOs and DESs will maintain and update a monthly roster of current sex offenders names and provide it to the Sexual Assault Review Board; the Army Command PM and DES and the garrison commander.

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

(1) Complete a Raw Data File as an information entry into ALERTS.

(2) 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.

(f) DoD civilians, contractors, and family members that fail to register at the installation PMO/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.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016; 81 FR 78912, Nov. 10, 2016]

§ 635.7 Collection of deoxyribonucleic acid.

(a) Army Law Enforcement (LE) personnel will collect deoxyribonucleic acid (DNA) pursuant to DoDI 5505.14 (available at *http://www.dtic.mil/whs/directives/corres/pdf/550514p.pdf*), DNA Collection Requirements for Criminal Investigations. Per this subpart, 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 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 DoDI 5505.11 (available at *http://www.dtic.mil/whs/directives/corres/pdf/550511p.pdf*), Fingerprint Card and Final Disposition Report Submission Requirements, and 32 CFR part 310, Department of Defense Privacy Program, except for the listed violations that are exclusively military offenses. For the purposes of this rule, 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.

(1) 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.

(2) Army LE personnel will use the U.S. Army Criminal Investigation Laboratory (USACIL) DNA kit which includes a DNA sample card and the USACIL DNA database collection eform. Army LE personnel will forward civilian DNA samples to the USACIL. 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.

(c) DoD Instruction 5505.14 (available at *http://www.dtic.mil/whs/directives/corres/pdf/550514p.pdf*) 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 who were not convicted of any offense giving rise to the collection of DNA, do not submit requests to have their DNA record expunged through installation PMO/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.

Subpart B—Release of Information

§ 635.8 General.

(a) The policy of HQDA is to conduct activities in an open manner and provide the public accurate and timely information. Accordingly, law enforcement information will be released to the degree permitted by law and Army regulations.

(b) Any release of military police records or information compiled for law enforcement 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 military police records about themselves will be processed in compliance with FOIA and the Privacy Act.

(d) Military police records in the temporary possession of another organization remain the property of the originating law enforcement agency. The following procedures apply to any organization authorized temporary use of military police records:

(1) Any request from an individual seeking access to military police records will be immediately referred to the originating law enforcement agency for processing. The temporary custodian of military police records does not have the authority to release those records.

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

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

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.9 Release of information.

(a) Release of information from Army records to agencies outside DoD will be governed by 32 CFR part 518, 32 CFR part 505, AR 600–37, Unfavorable Information (Available at *http://www.apd.army.mil/pdffiles/r600_37.pdf*), and this part. Procedures for release of certain other records and information is contained in AR 20–1, Inspector General Activities and Procedures (available at *http://www.apd.army.mil/pdffiles/r20_1.pdf*), AR 27–20, Claims (available at *http://www.apd.army.mil/pdffiles/r27_20.pdf*), AR 27–40, Litigation (available at *http://www.apd.army.mil/pdffiles/r27_40.pdf*), AR 40–66, Medical Record Administration and Healthcare Documentation (available at *http://www.apd.army.mil/pdffiles/r40_66.pdf*), AR 195–2, Criminal Investigation Activities (available at *http://www.apd.army.mil/pdffiles/r195_2.pdf*), AR 360–1, The Army Public Affairs Program (available at *http://www.apd.army.mil/pdffiles/r360_1.pdf*), and AR 600–85, The Army Substance Abuse Program (available at *http://www.apd.army.mil/pdffiles/r600_85.pdf*). Installation drug and alcohol offices may be provided an extract of DA Form 3997 (Military Police Desk Blotter) for offenses involving the use of alcohol or drugs (for example, drunk driving, drunk and disorderly conduct, or positive urinalysis).

(b) Installation PM/DES are the release authorities for military police records under their control. They may release criminal record information to other activities as prescribed in 32 CFR part 518 and 32 CFR part 505, and this part.

(c) Authority to deny access to criminal records information rests with the initial denial authority (IDA) for the FOIA and the denial authority for Privacy Acts cases, as addressed in 32 CFR part 518 and 32 CFR part 505.

§ 635.10 Release of information under the Freedom of Information Act (FOIA).

(a) The release and denial authorities for all FOIA requests concerning military police records include PM/DES 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 public affairs officer prior to release of records under the control of the installation PM/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 32 CFR part 518 and as follows:

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

(2) Statutory and policy questions will be coordinated with the local staff judge advocate (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 Military Police Report or other military police records will be forwarded to the Director, USACRC, ATTN: CICR–FP, 27130 Telegraph Road, Quantico, VA 22134. The requestor will be informed that their 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 will 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 social security number, 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 the entire report, 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 will simply be forwarded to the Director, United States Army Crime Records Center (USACRC) for action.

(6) Requests for military police records that have been forwarded to USACRC and are no longer on file at the installation PMO/DES will 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 Director, USACRC address.

(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.

§ 635.11 Release of information under the Privacy Act of 1974.

(a) Military police records may be released according to provisions of the Privacy Act of 1974, 5 U.S.C. 552a, as implemented by 32 CFR part 310, DoD Privacy Program, 32 CFR part 505, The Army Privacy Program, and this part.

(b) The release and denial authorities for all Privacy Act cases concerning military police records are provided in § 635.9.

(c) Privacy Act requests for access to a record, when the requester is the subject of that record, will be processed as prescribed in 32 CFR part 505.

§ 635.12 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, non-judicial or administrative action is taken against the individual.

(b) In compliance with DoD policy, an individual will still remain entered in the Defense Clearance Investigations Index (DCII) to track all reports of investigation.

§ 635.13 Accounting for military police record disclosure.

(a) 32 CFR part 505 prescribes accounting policies and procedures concerning the disclosure of military police records.

(b) PM/DES will develop local procedures to ensure that disclosure of military police records as described in 32 CFR part 505 are available on request.

(c) In every instance where records are disclosed; individuals, agencies or components are reminded that use or further disclosure of any military police reports, Military Police Investigator (MPI) reports, or other information received must be in compliance with DoDI 5505.7 (available at *http://www.dtic.mil/whs/directives/corres/pdf/550507p.pdf*), 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.''

§ 635.14 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 32 CFR part 518 and 32 CFR part 505, federal statutes or executive orders.

(b) Release of U.S. information (classified military information or controlled unclassified information) to foreign governments is accomplished per AR 380–10 (available at *http://www.apd.army.mil/pdffiles/r380_10.pdf*).

Subpart C—Offense Reporting

§ 635.15 DA Form 4833 (Commander's Report of Disciplinary or Administrative Action) for Civilian Subjects.

Civilian Subjects titled by Army Law Enforcement. PM/DES and USACIDC will complete and submit disposition reports to USACRC for civilian subjects, not subject to the UCMJ, who are titled by Army law enforcement. PM/DES and USACIDC will complete the DA Form 4833 and submit the form to USACRC for these subjects. PM/DES and USACIDC will not include these completed DA Form 4833 for civilian personnel in reporting compliance statistics for commanders. This ensures records of dispositions of civilian subjects titled by military LE are available in CJIS to support NCIC background checks for firearms purchases, employment, security clearances etc.

§ 635.16 Fingerprint Card and Final Disposition Report Submission Requirements.

(a) *General.* This paragraph implements DoDI 5505.11, Fingerprint Card and Final Disposition Report Submission Requirements, which prescribes procedures for Army LE to report offender criminal history data, by submitting FBI Form FD 249 (Suspect Fingerprint Card) to USACRC. USACRC forwards this data to the Criminal Justice Information Services (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.

(b) Installation PM/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 civilians investigated for offenses equivalent to those listed in DoDI 5505.11. 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 (Available at *http://www.dtic.mil/whs/directives/corres/pdf/552511p.pdf*), Criminal Jurisdiction Over Civilians Employed By or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members.

(c) For purposes of this paragraph commanders will notify their installation PMO/DES 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 DoDI 5525.11 (available at *http://www.dtic.mil/whs/directives/corres/pdf/552511p.pdf*), Enclosure 2, or punishable pursuant to the U.S.C.

§ 635.17 Release of domestic incidents reports to the Army Family Advocacy Program (FAP).

(a) Installation PM/DES will comply with the reporting requirements set forth in AR 608–18 (available at *http://www.apd.army.mil/pdffiles/r608_18.pdf*).

(b) In addition to substantiated incidents of domestic violence, installation PM/DES will notify the Family Advocacy Program Manager (FAPM) and Social Work Services (SWS) 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 PM/DES will ensure these notifications are recorded in the official military police journal in ALERTS. This is to:

(1) Establish a history of incidents that indicate an emerging pattern of risk of maltreatment/victimization to Soldiers and or Family members. See AR 608–18 for incidents that define maltreatment.

(2) Develop a trend history of unsubstantiated–unresolved incidents in order to prevent possible violence or maltreatment from occurring.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.18 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, Chapter 3, contains additional information about domestic violence and protective orders. AR 608–18, Glossary, Section II 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:

(1) A current or former spouse;

(2) A person with whom the abuser shares a child in common; or

(3) 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/DES.

§ 635.19 Protection Orders.

(a) A DD Form 2873, Military Protective Order (MPO) is a written lawful order issued by a commander that orders a Soldier to avoid contact with those persons identified in the order. MPOs 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 to the installation LE activity.

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

(1) The issuance of the protective order;

(2) The individuals involved in the order;

(3) Any change made in a protective order;

(4) The termination of the protective order.

(c) A Civilian Protective Order (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 the Armed Forces Domestic Security Act, 10 U.S.C. 1561a, 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.

§ 635.20 Establishing Memoranda of Understanding.

(a) Coordination between military law enforcement personnel and local civilian law enforcement personnel is essential to improve information sharing, especially concerning investigations, arrests, and prosecutions involving military personnel. PM/DES or other law enforcement officials shall seek to establish formal Memoranda of Understanding (MOU) with their civilian counterparts to establish or improve the flow of information between their agencies, especially in instances involving military personnel. MOUs can be used to clarify jurisdictional issues for the investigation of incidents, to define the mechanism whereby local law enforcement reports involving active duty service members will be forwarded to the appropriate installation law enforcement office, to encourage the local law enforcement 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 law enforcement agency and local civilian agencies.

(b) Installation commanders are authorized to contract for local, state, or federal law enforcement services (enforcement of civil and criminal laws of the state) from civilian police departments. (Section 120 of the Water Resources Development Act of 1976). 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) 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 U.S.C. 1561a).

(3) Procedures for responding to incidents that occur on the installation involving a civilian alleged offender.

(4) Procedures for local law enforcement to immediately (within 4 hours) notify the installation law enforcement office of incidents/investigations involving service members.

(5) Procedures for transmitting incident/investigation reports and other law enforcement information involving active duty service members from local civilian law enforcement agencies to the installation law enforcement office.

(6) Notification that a Solider is required to register as a sex offender either as the result of military judicial proceedings or civilian judicial proceedings.

(7) Procedures for transmitting civilian protection orders (CPOs) issued by civilian courts or magistrates involving active duty service members from local law enforcement agencies to the installation law enforcement office.

(8) Designation of the title of the installation law enforcement recipient of such information from the local law enforcement agency.

(9) Procedures for transmitting military protection orders (MPOs) from the installation law enforcement office to the local civilian law enforcement agency with jurisdiction over the area in which any person named in the order resides.

(10) Designation of the title of the local law enforcement agency recipient of domestic violence and CPO information from the installation law enforcement 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 the Privacy Act of 1974 (see 5 U.S.C. 552a(b)(7)).

(13) Regular meetings between the local civilian law enforcement agency and the installation law enforcement office to review cases and MOU procedures.

§ 635.21 Suspicious Activity Reporting (SAR).

(a) 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.

(b) 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.

(c) Any concerned soldier or citizen can submit a SAR to the nearest installation PMO/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.

Subpart D—Victim and Witness Assistance Procedures

§ 635.22 Procedures.

(a) As required by DoDD 1030.01 (Available at *http://www.dtic.mil/whs/directives/corres/pdf/103001p.pdf*), Army personnel involved in the detection, investigation, and prosecution of crimes must ensure that victims and witnesses rights are protected. Victim's 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) [Reserved]

Subpart E—National Crime Information Center Policy

§ 635.23 Standards.

The use of NCIC 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/Garrison Commander as set forth in DoD 5200.08–R (Available at *http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf*) and DoDI 5200.08 (Available at *http://www.dtic.mil/whs/directives/corres/pdf/520008p.pdf*). Visitors to Army installations are non-DoD affiliated personnel.