AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

635.17 Release of domestic incidents reports to the Army Family Advocacy Program (FAP).
635.18 Domestic violence.
635.19 Protection Orders.
635.20 Establishing Memoranda of Understanding.
635.21 Suspicious Activity Reporting (SAR).

Subpart D—Victim and Witness Assistance Procedures

635.22 Procedures.

Subpart E—National Crime Information Center Policy

635.23 Standards.

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