AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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