Office of the Secretary of Defense

§ 329.3

(j) Routine Use—Disclosure to Military Banking Facilities Overseas. Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

(k) Routine Use—Disclosure of Information to the General Services Administration (GSA). A record from a system of records maintained by this component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(l) Routine Use—Disclosure of Information to the National Archives and Records Administration (NARA). A record from a system of records maintained by this component may be disclosed as a routine use to the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

(m) Routine Use—Disclosure to the Merit Systems Protection Board. A record from a system of records maintained by this component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

(n) Routine Use—Counterintelligence Purpose. A record from a system of records maintained by this component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

PART 329—NATIONAL GUARD BUREAU PRIVACY PROGRAM

Sec. 329.1 Purpose.
data accurate, relevant, timely, and/or complete.

Appellate authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where a person other than authorized users (with an official need to know), and for an other than authorized purpose has access or potential access to personally identifiable information, whether physical or electronic. A breach can include identifiable information in any form. (As defined by DoD Director of Administration and Management Memo. 5 Jun 2009 entitled “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).”) (Available at http://www.dod.mil/pubs/foi/privacy/docs/DA_M6_5_2009Responding_toBreach_of_PII.pdf)

Chief, National Guard Bureau (CNGB). A principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, on matters involving non-federalized National Guard forces and on other matters as determined by the Secretary of Defense; and the principal adviser to the Secretary of the Army and the Chief of Staff of the Army, and to the Secretary of the Air Force and the Chief of Staff of the Air Force, on matters relating to the National Guard, the Army National Guard of the United States, and the Air National Guard of the United States. The CNGB also represents the National Guard on the Joint Chiefs of Staff.

Completeness. All elements necessary for making a determination are present before such determination is made.

Computer matching program. A program that matches the personal records in computerized database of two or more Federal agencies.

Denial authority. The individual with authority to deny requests for access or amendment of records under 5 U.S.C. 552a.

Determination. Any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Directorate/Division. The terms directorate and division are used to refer to suborganizations within the NGB. The Joint Staff and Air Guard Readiness Center uses the term “Directorate” to refer to their suborganizations and the Army Guard Readiness Center uses the term “Division” to refer to their suborganizations.

Disclosure. Giving information from a system, by any means, to anyone other than the record subject.

Disclosure accounting. A record of all disclosures made from a SOR, except for disclosures made to Department of Defense personnel for use in performance of their official duties or disclosures made as required by 5 U.S.C. 552.

Federal Register (FR). A daily publication of notices and rules issued by Federal Agencies and the President printed on a daily Federal weekday.

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence. (As defined by 5 U.S.C. 552a)

Maintain. Maintain, collect, use or disseminate. (As defined by 5 U.S.C. 552a)

Memorandum of Agreement. A written understanding (agreement) between parties to cooperatively work together on an agreed upon project or meet an agreed objective.

Memorandum of Understanding. A written agreement between parties describing a bilateral or multilateral agreement between parties.

Necessary. A threshold of need for an element of information greater than mere relevance and utility.

Personal information. Information about an individual other than items of public record.

Personally Identifiable Information (PII). Personal information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her. Information which can be used to distinguish or trace an individual’s identity which is linked or linkable to a specified individual.

Privacy Act (5 U.S.C. 552a) Request. An oral (in person) or written request by an individual to access his or her records in a SOR.
Privacy Act (5 U.S.C. 552a) Statement (PAS). A statement given to an individual when soliciting personal information that will be maintained in a SOR that advises them of the authority to collect information, the principal purpose(s) that the information will be used for, the routine uses on how the information will be disclosed outside of the agency, and whether it is mandatory or voluntary to provide the information and any consequences for not providing the information.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new SOR is being created under 5 U.S.C. 552a. Privacy Impact Assessments are required for all information systems and electronic collections that collect, maintain, use, or disseminate personally identifiable information about members of the public (this includes contractors and family members), under Public Law 107–347, Section 208 of the E-Government Act of 2002. DoD Regulation 5400.16–R, entitled “Department of Defense Privacy Impact Assessment (PIA)” (Available at http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf), provides additional requirements for PIAs, including a requirement to write a PIA on any information systems or electronic collection of PHI on Federal personnel.

Protected Health Information (PHI). Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual’s education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph (As defined by 5 U.S.C. 552a).

Relevance. Limitation to only those elements of information that clearly bear of the determination(s) for which the records are intended.

Routine use. The disclosure of a record outside the DoD for a use that is compatible with the purpose for which the information was collected and maintained by the DoD. The routine use must be included in the published system notice for the SOR involved. The DoD Blanket Routine Uses, found in 32 CFR part 310, Appendix C are applicable to all SORNs published by DoD.

System Manager. The official who is responsible for managing a SOR, including policies and procedures to operate and safeguard it. Local System Managers operate record systems or are responsible for the records that are maintained in decentralized locations but are covered by a SORN published by another DoD activity or a Government-Wide SORN.

System of Records (SOR). A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Notice (SORN). The official public notice published in the FR of the existence and content of the SOR. As required by 5 U.S.C. 552a and 32 CFR part 310, appendix E. The notice shall include:

(1) System ID.
(2) The name and location of the system.
(3) The categories of individuals on whom records are maintained in the system.
(4) The categories of records maintained in the system.
(5) Each routine use of the records contained in the system, including the categories of users and the purpose of such use.
(6) The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.
(7) The title and business address of the agency official who is responsible for the SOR.
(8) The agency procedures whereby an individual can be notified at his request if the SOR contains a record pertaining to him.
§ 329.4 Policy.

In accordance with 32 CFR part 310, it is NGB’s policy that:

(a) Personal information contained in any SOR maintained by any NGB organization will be safeguarded to the extent authorized by 5 U.S.C. 552a, Appendix I of Office of Management and Budget Circular No. A–130, and any other applicable legal requirements.

(b) NGB will collect, maintain, use, and disseminate personal information only when it is relevant and necessary to achieve a purpose required by a statute or Executive Order.

(c) NGB will collect personal information directly from the individuals to whom it pertains to the greatest extent possible and will provide individuals a PAS at the time of collection when the information being collected will be filed and/or retrieved by the subject’s name or other unique identifier. The PAS will contain the following elements, as required by 5 U.S.C. 552a:

(1) The statutory authority or Executive Order that allows for the solicitation,

(2) The intended use/purpose that will be made of the information collected,

(3) The routine uses that may be made of the information collected; and

(4) Whether it is mandatory or voluntary for the individual to disclose the requested information and the non-punitive effects on the individual for not providing all or any part of the requested information. Collection can only be mandatory if the statutory authority or Executive Order cited provides a penalty for not providing the information.

(d) NGB offices maintaining records and information about individuals will ensure that such data is protected from unauthorized access, use, dissemination, disclosure, alteration, and/or destruction. Offices will establish safeguards to ensure the security of personal information is protected from threats or hazards that might result in substantial harm, embarrassment, inconvenience, or unfairness to the individual using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, appendix A, and DoD Manual (DoDM) 5200.01, Volume 4, entitled “DoD Information Security Program: Controlled Unclassified Information (CUI).”

(e) NGB offices shall permit individuals to access and have a copy of all or any portion of records about them, unless an exemption for the system has been properly established (see 5 U.S.C. 552a, 32 CFR part 310, subparts D and F, and §329.7 of this part). Individuals requesting access to their record will also receive concurrent consideration under 5 U.S.C. 552 and 32 CFR part 286.

(f) NGB offices will permit individuals an opportunity to request that records about them be corrected or amended (see 5 U.S.C. 552a, 32 CFR part 310, subpart D, and §329.6 of this part).

(g) Any records about individuals that are maintained by the NGB will be maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual before making any determination about the individual or before making the record available to any recipient pursuant to a routine use.

(h) NGB will keep no record that describes how individuals exercise their rights guaranteed by the First Amendment, unless expressly authorized by statute or by the individual to whom the records pertain, or is pertinent to and within the scope of an authorized law enforcement activity.

(i) NGB will notify individuals whenever records pertaining to them are made available under compulsory legal processes, if such process is a matter of public record.

(j) NGB will assist individuals in determining what records pertaining to them are being collected, maintained, used, or disseminated.