(k) NGB offices and personnel, including contractors, maintaining and having access to records and information about individuals will manage them and conduct themselves so as to avoid the civil liability and criminal penalties provided for under 5 U.S.C. 552a.

§ 329.5 Responsibilities.

(a) *Chief of the National Guard Bureau (CNGB)*. The CNGB, under the authority, direction, and control of the Secretary of Defense (SecDef), approves and establishes overall policy, direction, and guidance for the NGB privacy program and promulgates privacy policy for the non-Federalized National Guard.

(b) *NGB Chief Counsel*. The NGB Chief Counsel, under the authority, direction, and control of the CNGB, shall:

(1) Serve as the National Guard Component Senior Official for Privacy (CSOP) pursuant to part 32 CFR part 310, subpart A.

(2) Direct and administer the Privacy Program for the NGB as well as the National Guard of the States, Territories, and the District of Columbia as it pertains to the maintenance of records protected by 5 U.S.C. 552a, other Federal laws on privacy, and OMB and DoD Privacy policies.

(3) Ensure implementation of and compliance with standards and procedures established by 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, and this part.

(4) Serve as the appellate authority on denials of access or amendment.

(5) Direct the implementation all aspects of 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(c) *Chief of the Office of Information and Privacy (OIP)*. The Chief of the OIP, under the authority, direction, and control of the NGB Chief Counsel, shall:

(1) Oversee the National Guard's compliance with 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, this part, and other Federal laws on privacy, and OMB and DoD Privacy policies.

(2) Issue policy and guidance as it relates to 5 U.S.C. 552a and other Federal and DoD Privacy requirements.

(3) Collect, consolidate, and submit Privacy reports to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service (Air Force or Army) that the reporting of information pertains to. This includes, but is not limited to:

(i) Personally Identifiable Information (PII) Breach Reports required by 32 CFR part 310, subpart B,

(ii) Quarterly Training Reports, SORN Reviews, and Privacy Complaints; and,

(iii) Reports pursuant Public Law 17–347.

(4) Submit all approved SORNs to the DPCLO or the respective service that has the statutory authority to publish the SORN for publication in the FR.

(5) Refer inquiries about access, amendments of records, and general and specific exemptions listed in a SORN to the appropriate System Manager.

(6) Review all instructions, directives, publications, policies, Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), data sharing agreements, data transfer agreements, data use agreements, surveys (including web-based or electronic), and forms that involve or discuss the collection, retention, access, use, sharing, or maintenance of PII are to ensure compliance with this part.

(7) Make training resources available to NGB personnel, including contractors, regarding 5 U.S.C. 552a, OMB A–130, 32 CFR part 310, compliance with this part, and other Federal and DoD Privacy requirements.

(d) *Chief of Administrative Law*. The Chief of Administrative Law shall serve as the initial denial authority (IDA) to deny official requests for access or amendment to an individual's record pursuant to a published NGB SORN under 5 U.S.C. 552a or amendments to such records.

(e) *Chief of Litigation and Employment Law*. The Chief of Litigation and Employment Law will notify the Chief of the OIP of any complaint citing 5 U.S.C. 552a is filed in a U.S. District Court against the NGB, or any employee of NGB using the procedures outlined in § 329.6 of this part.

(f) *NGB Comptroller/Director of Administration and Management (DA&M)*. The

NGB Comptroller/DA&M shall ensure appropriate Federal Acquisition Regulation (FAR) (Available at *https://www.acquisition.gov/far/*) and Defense Federal Acquisition Regulation Supplement (DFARS) (Available at *http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html*) clauses (FAR Subpart 24.1 related to 5 U.S.C. 552a and FAR subpart 24.2 related to 5 U.S.C. 552, as well as DFARS clauses 52.224–1 and/or 52.224–2) are included in all contracts that provide for contractor personnel to have access or maintain records, including records in information systems, that are covered by 5 U.S.C. 552a or that contain PII.

(g) *NGB Directorates/Divisions.* All NGB directorates/divisions maintaining records containing PII or that have personnel that have access to PII shall:

(1) Ensure that a SORN is published in the FR before collection of any information subject to 5 U.S.C. 552a is scheduled to begin.

(2) Ensure System Managers comply with all responsibilities outlined in paragraph (h) of this section. This includes referring any proposed denials of access or amendment under 5 U.S.C. 552a to the Chief of the OIP within 10 working days.

(3) Evaluate Privacy requirements for information systems and electronic collection or maintenance of PII in the early stages of system acquisition/development. This includes completing a PIA in accordance with the requirements of Public Law 107–347, section 208 of the E-Government Act of 2002, and DoD 5400.16–R.

(4) Ensure personnel, including contractors, who have access to PII complete appropriate Privacy training as required by 5 U.S.C. 552a, 32 CFR part 310, subpart H, and Part II of DoD Policy ''Safeguarding Against and Responding to Breaches of PII'' (*http://www.dod.mil/pubs/foi/privacy/docs/DA_M6_5_2009Responding_toBreach_of_PII.pdf*) as follows:

(i) Orientation Training: Training that provides individuals with a basic understanding of the requirements of 5 U.S.C. 552a as it applies to the individual's job performance. The training is for all personnel, as appropriate, and should be a prerequisite to all other levels of training.

(ii) Specialized Training: Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, information technology professionals, and any other personnel responsible for implementing or carrying out functions under this part.

(iii) Management Training: Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the Privacy program.

(iv) Privacy Act (5 U.S.C. 552a) SOR Training: All individuals who work with a Privacy Act (5 U.S.C. 552a) SOR are trained on the provisions of the 5 U.S.C. 552a SORN(s) they work with, 32 CFR part 310, and this part.

(5) Ensure all instructions, directives, publications, policies, MOAs, MOUs, data sharing agreements, data transfer agreements, data use agreements, surveys (including Web-based or electronic surveys), and forms that involve the collection, retention, use, access, sharing, or maintenance of PII are coordinated with the Chief of the OIP.

(6) Ensure that any suspected or confirmed breaches of PII, or potential breaches of PII, are immediately reported to the Chief of the OIP in accordance with NGB Memorandum 380–16/33–361. (Available at *http://www.nationalguard.mil/sitelinks/links/NGB%20Memorandum%20380-16%2033-361,%20PII%20Incident%20Response%20Handling.pdf*).

(7) Ensure policies and administrative processes within their directorates are evaluated to ensure compliance with the procedures in this part.

(h) *System Managers.* System Managers will:

(1) Report any changes to their existing SORN(s) to the Chief of the OIP for publishing in the FR at least 90 working days before the intended change to the system.

(2) Review their published SORN(s) on a biennial basis and submit updates to the Chief of the OIP as necessary.

(3) Ensure appropriate training is provided for all users, to include contractors, which have access to records covered by their published system notice.

(4) Ensure safeguards are in place to protect all records containing PII (electronic, paper, etc.) from unauthorized access, use, disclosure, alteration, and/or destruction using guidelines found in 32 CFR part 310, subpart B, 32 CFR part 310, appendix A, and DoDM 5200.01, Volume 4.

(5) Assist in responding to any complaints and inquiries regarding the collection or maintenance of, or access to information covered by their published SORN(s).

(6) Process all 5 U.S.C. 552a requests for access and amendment, as outlined in § 329.6 of this part.

(7) Maintain a record of disclosures for any records covered by a SORN using a method that complies with 32 CFR part 310, subpart E when disclosing records outside of the agency (DoD). Such disclosures will only be made when permitted by a Routine Use published in the SORN.

(i) As required by 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will be maintained for 5 years after the disclosure, or for the life of the record, whichever is longer. The record may be maintained with the record disclosed, or in a separate file within the office's official record keeping system.

(ii) Pursuant to 5 U.S.C. 552a and 32 CFR part 310, subpart E, the disclosure accounting will include the release date, a description of the information released, the reason for the release; and, the name and address of the recipient.

§ 329.6 Procedures.

(a) *Publication of notice in the FR.* (1) A SORN shall be published in the FR of any record system meeting the definition of a SOR, as defined by 5 U.S.C. 552a.

(2) System Managers shall submit notices for new or revised SORNs through their Director to the Chief of the OIP for review at least 90 working days prior to implementation.

(3) The Chief of the OIP shall forward complete SORNs to the Defense Privacy and Civil Liberties Office (DPCLO), or the respective service that has the statutory authority to publish the SORN, for review and publication in the FR in accordance with 32 CFR part 310, subpart G. Following the OMB comment period, the public is given 30 days to submit written data, views, or arguments for consideration before a SOR is established or modified.

(b) *Access to Systems of Records Information.* (1) As provided by 5 U.S.C. 552a, records shall be disclosed to the individual they pertain to and under whose individual name or identifier they are filed, unless exempted by the provisions in 32 CFR part 310, subpart F, and § 329.7 of this part. If an individual is accompanied by a third party, or requests a release to a third party, the individual shall be required to furnish a signed access authorization granting the third party access conditions according to 32 CFR part 310, subpart D.

(2) Individuals seeking access to records that pertain to themselves, and that are filed by their name or other personal identifier, may submit the request in person, by mail, or by email. All requests for access must be in accordance with these procedures:

(i) Any individual making a request for access to records in person shall show personal identification to the appropriate System Manager, as identified in the SORN published in the FR, to verify his or her identity, according to 32 CFR part 310, subpart D.

(ii) Any individual making a request for access to records by mail or email shall address such request to the System Manager. If the System Manager is unknown, the individual may inquire to NGB–JA/OIP: AHS-Bldg 2, Suite T319B, 111 S. George Mason Drive, Arlington, VA 22204–1382, or email *ng.ncr.arng.mbx.ngb-privacy-office@mail.mil* for assistance in locating the System Manager.

(iii) Requests for access shall include a mailing address where the records should be sent and include either a signed notarized statement or a signed unsworn declaration to verify his or her identity to ensure that they are