

Department of the Army
Headquarters, U.S. Army Garrison
462 Hamilton Road, Suite 120
Fort Sill, Oklahoma 73503
8 August 2012

*Fort Sill Supplement 1 to AR 340-21

Office Management
THE ARMY PRIVACY PROGRAM

Summary. This publication prescribes policies and guidance for privacy issues.

Applicability. This publication applies to all Fort Sill garrison agencies.

Suggested Improvements. The proponent of this supplement is the Directorate of Human Resources (DHR). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to DHR, Administrative Services Division (ASD), 4700 Mow-Way Road, Suite G06, Fort Sill, OK 73503.

Distribution. This publication is distributed solely through the DHR, ASD Homepage at <http://sill-www.army.mil/USAG/publications2012.html>.

*This publication supersedes Fort Sill Supplement 1 to AR 340-21, The Army Privacy Program, 9 July 2009.

AR 340-21, 5 July 1985, is further supplemented as follows:

- 1. Purpose.** This publication prescribes policies and guidance for privacy issues as it pertains to garrison activities.
- 2. References.** Required and related publications and forms are listed in appendix A.
- 3. Explanation of Abbreviations and Terms.** Abbreviations and terms used in this regulation are explained in the glossary.

Paragraph 1-4. Responsibilities. Add subparagraphs f and g after subparagraph e:

f. The Director of Human Resources will designate appoint an individual as the Garrison Privacy Act Official.

g. Heads of Fort Sill special staffs, directorates, and support offices listed in appendix A are responsible for—

(1) Designating a Privacy Act Coordinator for their organization and elements under their jurisdiction. Directors, chiefs will send a copy of the duty appointment, which

includes name, rank, office, telephone number, and e-mail address to DHR, ASD, Garrison Privacy Act Official.

(2) Coordinating with the Garrison Privacy Act Official before dispatching command correspondence, directives, and/or publications which implement any Privacy Act provisions.

(3) Processing verbal and written (formal) Privacy Act requests received from individuals.

(a) Activities will, upon receipt of a verbal Privacy Act request from an employee, provide access to and/or a copy of documents being maintained on them that are in a Privacy Act System of Records (i.e., supervisor's employee file).

(b) Activities will, upon receipt of a written Privacy Act request from an employee, send such request to the Garrison Privacy Act Official for processing.

(c) Activities will send any requests to deny an employee access to his/her records to the Garrison Privacy Act Official for processing. No individual on Fort Sill has the authority to deny an employee access to his/her records. Only the appropriate Access and Amendment Refusal Authority (AARA) has this authority.

(4) Reviewing requests for private data from other agencies to ensure they demonstrate the "need-to-know" requirement, in order to perform their job prior to releasing the data to them.

(5) Reviewing agency documents/data placed on "P" and/or "S" drives and folders shared on personal computers drives quarterly for private data. NOTE: Network Enterprise Center (NEC) server administrative personnel and the Garrison Privacy Act Official are authorized access to "S" drives.

(a) If no private data is found, the Privacy Act Coordinator will submit a report to the Garrison Privacy Act Official indicating the date they conducted the review and that no private data was found.

(b) If private data is found and the data is properly safeguarded (i.e., only individuals with a need-to-know have access to the data and only their names are included in the properties of the folder), the Privacy Act Coordinator will submit a report to the Garrison Privacy Act Official indicating what data is stored on the "S" drive and that it is properly safeguarded.

(c) If private data is found and the data is not properly safeguarded, the Privacy Act Coordinator will document the date and time the private data was found, where the data was located (include the path to the document (i.e., the names of the folders you accessed to get to the document) and the documents found, and then remove the data. The PA Coordinator will report their findings to the agency head and provide a copy of

the report to the Garrison Privacy Act Official. Privacy Act data can be restored to the “S” drive after safeguards have been put in place (see paragraph (b) above).

(6) Immediately upon receipt of notice of loss of Personally Identifiable Information (PII), provide notice to [US-CERT at http://www.us-cert.gov](http://www.us-cert.gov) and piireporting@us.army.mil within one hour of discovery. At the same time, provide a report to the Garrison Privacy Act Official. This report must include the type of data lost and the number of individuals affected. The Garrison Privacy Act Official will provide further instructions after receipt of this report.

(7) Ensuring Privacy Act data is safeguarded during transmittals. Place the appropriate cover sheet on the information when removing data from file, prior to placing data in messenger envelopes (shotguns), prior to mailing the data, and encrypting electronic mail that contains Privacy Act data.

(8) Ensuring their local forms, for which they are the proponent and the form is requesting Privacy Act data, has a Privacy statement within the body of the form. Agencies may create their own blank forms; however, they must submit proposed forms or updates to existing forms to the DHR, ASD Forms Manager for approval. Use a DD Form 67 (Form Processing Action Request) to submit the form to the Forms Manager.

Paragraph 1-9. Privacy Official. Add subparagraph c after subparagraph b.

c. The Privacy Act Coordinator will perform those duties of privacy officials as outlined in paragraph 1-9.

Paragraph 3-1. Disclosure of Personnel Information to other Agencies and Third Parties. Add the following after last sentence of subparagraph a.

The proponent of the requested document must determine if the requester has a need for the requested data. The placement of private data in shared folders on “P” and “S” drives and folders on a personal computer can violate this provision. Not everyone that has access to a shared folder meets the “need-to-know to perform their duties” requirement on each document placed in the folder.

Appendix A References

Section I Required Publications

AR 340-21
The Army Privacy Program

Section II Related Publications

This section contains no entries.

Section III Prescribed Forms

DA Form 2028
Recommended Changes to Publications and Blank Forms

Section IV Referenced Forms

This section contains no entries.

Glossary

Section I Abbreviations

AARA

Access and Amendment Refusal Authority

AR

Army Regulation

ASD

Administrative Services Division

DA

Department of the Army

DHR

Directorate of Human Resources

PII

Personally Identifiable Information

IMWE-SIL-HRA



PAUL S. HASSENLOPP
COL, FA
Garrison Commander

JAMES A. MILLER
Director of Human
Resources

DISTRIBUTION:
Fort Sill Intranet