DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT SILL
462 HAMILTON ROAD, SUITE 120
FORT SILL, OKLAHOMA 73503

IMSI-ZA

17 September 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Privacy Act Policy, GC Policy Memorandum 20-04

1. Purpose: We are responsible for ensuring our privacy practices and procedures are followed. Privacy is everyone's responsibility. The Privacy Act promotes and safeguards Personally Identifiable Information (PII) maintained in a system of record. It's our job to ensure collection, storage, use, maintenance, processing, dissemination, and disclosure of PII adheres to statutory and regulatory compliance standards in accordance with (5 U.S.C. § 552a, 32 CFR 310).

2. Scope: This policy is applicable to all military, Civilian, and contractor personnel assigned to or under the operational control of the Fort Sill Garrison.

3. Policy:

a. Any PII collection must be coordinated with the Privacy Office for approval prior to use or if currently being used to ensure compliance. Additional requirements may include Privacy Impact Assessment (PIA), Privacy Policy or Notice, Privacy Act Statement, or System of Records Notice (SORN).

b. All suspected or actual breaches must be reported within one hour of discovery. Report incidents, whether suspected or confirmed, to United States Computer Emergency Readiness Team (US-CERT). Simultaneously, an email will be sent to the Records Management and Declassification Agency (RMDA) which notifies Army leadership that an initial report has been submitted. Lastly, contact your Privacy Act Officer. Notifications will include:

(1) Notify US-CERT within one hour at https://www.us-cert.gov.

(2) Notify Army FOLA/PA Office within 24 hours at https://www.privacy.army.mil/PATS/.

(3) Notify Regional Computer Emergency Response Team (RECERT) & Army Computer Emergency Response Team (ACERT) for possible compromise of Army Networks.

(4) Determine nature of breach and type by assessing Low/Moderate/High Risk or Harm.

(5) For individual notifications, see Sample notification letter at https://www.rmda.army.mil/priacy/RMDA-PO-Infractions.html.

4. Employees must only collect the minimum amount of PII that is legally authorized and necessary to support mission requirements.

5. We must ensure the security and confidentiality of information and records be protected against possible threats or hazards and permit access only to authorized persons. All records (paper and electronic) will be protected as prescribed in DOD Regulation 5400.11-R (DOD Privacy Program) and AR 25-22 (The Army Privacy Program).

6. Individuals who perceive an alleged violation or want to file a complaint, should contact the points of contact below.

7. The points of contact for this policy is the Garrison Privacy Official, Mr. Anthony Montero, (580) 442-6573 (anthony.x.montero.civ@mail.mil).

8. This GC Policy memorandum supersedes GC Policy Memorandum, 19-03, Subject: Privacy Act Policy, GC Policy Memorandum 19-03, 10 January 2020.

RHETT A. TAYLOR
COL, FA
Commanding

DISTRIBUTION:
Fort Sill Intranet
HQ Garrison
DES
DHR
DPTMS
DPW
DFMWR
PAIO
RMO
Safety Office