DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND
US ARMY GARRISON ROCK ISLAND ARSENAL
1 ROCK ISLAND ARSENAL
ROCK ISLAND, ILLINOIS 61299-5000

IMRI-ZA JUN 2 0 2016

MEMORANDUM FOR All US Army Garrison Rock Island Arsenal (USAG RIA) Employees

SUBJECT: Protecting Personally Identifiable Information (PII) and PII Breach Notification – Policy Memorandum #B-19

1. References:

a. Privacy Act of 1974: http://www.usdoj.gov/oip/privstat.htm.

b. Department of Defense (DoD) Privacy Act Program, DoD 5400.11-R, 14 May 2007: http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf.

c. Department of Defense Directive (DoDD) 5400.11, 8 May 2007.

d. DoD Memorandum, "DoD Guidance on Protecting Personally Identifiable Information (PII)," 18 August 2006.

e. Office of the Secretary of Defense (OSD) Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information", 21 September 2007.

f. DoD Freedom of Information Act Program, DoD 5400.7-R, September 1998.

g. Information Security Program, DoD 5200.1-R, January 1997.

h. Department of the Army Freedom of Information Act Program, Army Regulation (AR) 25-55, 1 December 1997.

i. The Army Records Information Management System (ARIMS), AR 25-400-2, 2 October 2007.

j. Army Records Management & Declassification Agency (RMDA): https://www.rmda.army.mil/ORGANIZATION/pa.shtml.

2. Purpose. The publication of this memorandum implements the Garrison policy regarding the protection of PII for Garrison employees and PII breach notification in accordance with DoD policy and guidance. The purpose of the policy is to ensure that all Garrison personnel understand and execute their responsibilities to protect PII. PII is

all information that can be used by any person to distinguish, trace or identify another individual. This type of information may be obtained from users through online forms and can include your mailing address, credit card number, phone number, e-mail, social security number or any other unique identifier. Other types of PII include biometric records, mother's maiden name, education, financial transactions, medical history, place and date of birth, criminal or employment history and information which can be used to uniquely identify an individual. Additional topics covered by this policy include other sensitive private data related to health, education, medical conditions, private relationships and marital status.

3. Applicability. This policy is effective immediately and applies to all Garrison personnel and supporting Contractors.

4. Policy. It is Garrison Information Assurance policy that:

a. The privacy of an individual is a personal and fundamental right that will be respected and protected.

b. Appropriate administrative, technical and physical safeguards will be maintained to ensure the security and confidentiality of PII of current and former Garrison personnel and to protect against any comprise which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual where information is stored or transferred in either hardcopy or electronic form.

c. Appropriate safeguards will be maintained to ensure the physical security of Government Information Systems (IS), e.g., laptop computers, external hard disk drives and Compact Disks (CDs), etc. This is particularly important when taking IS away from the workplace. Personnel shall secure IS at all times when not in use and in their possession.

d. Any computer connecting to a Government unclassified network must be Common Access Card (CAC) enabled. CAC enabled means that the computer is equipped with a reader and associated software to use the CAC. The CAC provides strong assurance that users possess appropriate credentials to access the network. The CAC is also used to encrypt and digitally sign e-mail messages to ensure sensitive information such as PII is protected and to authenticate the identity of the sender.

e. Individuals who violate their responsibilities may be subject to adverse administrative, disciplinary or other actions. Managers/Supervisors may be subject to disciplinary action for failure to adequately instruct, train or supervise employees in their responsibilities related to PII, and/or failure to take appropriate action upon discovering a breach or failure to take the required steps to prevent a breach from occurring. For

this policy, suspected loss, actual loss or compromise of PII will be referred to as a breach. A breach or compromise incident occurs when it is suspected or confirmed that PII is lost, stolen or otherwise made available to individuals without a duty-related official need to know.

5. Responsibilities.

a. The leader/supervisor of each Garrison Directorate will:

(1) Ensure that personnel complete annual web-based PII training and are adequately instructed in their responsibilities related to PII.

(2) Appoint, in writing, a primary and alternate Privacy Coordinator (PC) whose duties will be to ensure the protection of PII within their organization. A copy of the appointment letter will be provided to the Garrison Privacy Officer.

(3) Ensure that compromised PII is reported to the Garrison Privacy Officer as soon as the breach is discovered.

b. Subordinate supervisors will:

(1) Ensure that their employees are adequately instructed in their responsibilities related to PII.

(2) Review all requests to remove copies, not originals, of PII from the workplace following PC review and recommendation. PII originals shall not be taken from the workplace. The Supervisor will also determine the length of time that copies of PII may be removed from the workplace.

(3) Report compromised PII to the head of the organization.

c. Privacy Coordinators will:

(1) Print copies of the DA Label 87 "For Official Use Only" cover sheet and make them accessible to office personnel who handle PII within their organization.

(2) Review holdings of PII as part of the quarterly PII inspection and unannounced inspections.

(3) Determine whether the use of Social Security Numbers (SSNs) is redundant in work processes, data calls or surveys and is reduced or alternatively replaced as a personal identifier as a master control program initiative.

(4) Assign high, moderate or low PII impact categories to electronic and hardcopy records in accordance with DoD policy (reference 1e).

(5) Establish logging and tracking procedures for High Impact Electronic PII on portable devices and sign them out at the time of removal from the workplace. (This may be as simple as creating a spreadsheet with the date, time, type of PII contained on the device, name of the employee removing it from the workplace and the date and time when it is returned.)

(6) Evaluate all requests to remove copies, (not originals) of PII from the workplace and make appropriate recommendations to the approving supervisor.

d. Information Assurance Support Officers (IASOs) within organizations will ensure their organization's government-owned laptops and USB flash drives (if authorized) are protected with encryption software. Refrain from storing PII on disks, CDs, USB flash drives, memory sticks, flashcards, or any other media that may, from time to time be authorized, unless the material is encrypted and favorable recommendation from the PC and Supervisory approval are obtained. Government PII should never be stored on personally-owned notebooks, desktops, flash drives, etc. Mark all government provided equipment containing PII records appropriately "For Official Use Only (FOUO) – Privacy Act Data".

e. Garrison Military and Civilian personnel and supporting Contractors will:

(1) Complete annual web-based mandatory training on "Privacy Act: Protecting Personal Information" as provided. Upon completion, the trainee will print a certificate signifying acknowledgement of and accountability for the responsibilities, procedures, violations and penalties associated with handling and mishandling PII.

(2) Handle Privacy Act data as FOUO.

(a) Mark it when it is created or received as "FOUO – Privacy Act of 1974".

(b) Place FOUO markings at the bottom of the front cover, title page, on each page containing FOUO information and on the back cover (if any). Within a classified document, the page that contains classified and FOUO information will be marked with the highest classification markings on the top and bottom. If an individual page of a classified document contains only FOUO information, the page will be marked FOUO at the bottom of the page. PII transmitted outside DoD requires application of an expanded marking to explain the significance of the FOUO marking. This is accomplished by typing or stamping the following statement on the record prior to

transfer: "This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemptions Apply.

(c) Refrain from storing PII on disks, CDs, USB flash drives, memory sticks, flashcards, or any other media that may, from time to time, be authorized, unless the material is encrypted and favorable recommendation from the PC and Supervisory approval are obtained. Government PII should never be stored on personally-owned notebooks, desktops, flash drives, etc. Mark all government provided data storage equipment containing PII records appropriately: "For Official Use Only (FOUO) – Privacy Act Data".

(d) Cover or place PII in an out-of-sight location when those without an official need to know enter the work space.

(e) Remove the DoD CAC from the computer's CAC reader before stepping away from the work area, even for brief periods, to ensure protection of PII.

(f) Store PII to preclude unauthorized access during non-duty hours. PII must be stored in a locked desk, file cabinet or office that is not accessible during non-duty hours.

(g) Transport personal records containing PII with a DA Label 87 "FOUO" cover sheet and hand them to an authorized recipient. This is an official or an employee of a DoD component who has a need for the use of the information contained therein in the performance of their official duties (reference 1b). Receive PC recommendation and supervisory approval to transport PII on an authorized portable device.

(h) Mail PII with a DA Label 87 "FOUO" cover sheet sealed in an opaque envelope. The envelope shall be marked to an authorized recipient's attention but not marked with any reference to the material within it.

(i) Restrict discussions of PII over telephones with other Government agencies to a minimum and for official purposes only and not within areas where it may be overheard by those who do not have an official need to know.

(j) Cover all facsimile transmissions containing PII with a DA Label 87 "FOUO" cover sheet. The recipient will be alerted by e-mail or telephone that a fax containing PII is being sent. No faxes will be sent until the sender confirms that the recipient is aware of and awaiting the transmission.

(k) Mark e-mail messages to reflect that FOUO material is contained therein in both the opening line of text and each part of the message that contains PII. This will inform the recipient of limitations on further dissemination. Ensure there is an "official need to know" for each addressee, including "cc" addresses. Use DoD CAC to encrypt so that information, if compromised, is unusable by unauthorized individuals.

(l) Refrain from posting PII on publicly accessible DoD websites. PII posted on a public website is not protected and could enable identity theft to occur.

(m) Obtain a favorable recommendation from the PC, and then supervisory approval, before removing PII from the workplace. Copies, not originals of PII, should be removed only on a temporary basis and never stored permanently away from the work place.

(n) Dispose of PII records IAW AR 25-400-2, by any method that prevents inadvertent compromise, such as shredding using an approved shredder, burning, melting, chemical decomposition, pulping, pulverizing, or mutilation. PII must be unrecognizable and beyond reconstruction. Recycling contracts are acceptable, if the documents are properly protected while in a destruction bin, protected in transit and one of the above destruction methods is used by the contractor.

(o) Purge hard drives and magnetic media to permanently destroy PII information beyond recognition once the information is no longer required. Contact the Network Enterprise Center-Rock Island Arsenal for information.

(p) If records containing PII or PI are lost, stolen or compromised, the same shall be reported immediately to the employee's (or service member's) supervisor and the USAG RIA Privacy Officer, Ms. Joyce Rollins (Primary), DSN 793-1245, Commercial 309-782-1245, e-mail joyce.rollins.civ@mail.mil, or Ms. Julie Wheeler (Alternate), DSN 793-1320, Commercial 309-782-1320, e-mail julie.m.wheeler6.civ@mail.mil.

(q) The USAG RIA Privacy Officer will be responsible for determining whether there has been a breach of either PII or PI.

(r) In the event that the Garrison Privacy Officer determines that an actual or potential breach of PII or PI exists, the Garrison Privacy Officer shall determine the affected individual(s) and give notice to the affected individual(s) IAW DoD 5400.11-R (http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf).

(s) Teleworkers will implement appropriate physical, administrative and technical safeguards IAW appropriate telework policy and this policy to protect the security and confidentiality of PII.

6. Questions regarding this policy may be directed to the Garrison Legal Office POC, Ms. Carrie Schaffner, DSN 793-8444, Commercial 309-782-8444, or e-mail carrie.j.schaffner.civ@mail.mil.

KENNETH J. TAUKE
Colonel, MP
Garrison Commander

CF:
USAG RIA Supporting Contractor Personnel