DEPARTMENT OF THE ARMY
U.S. ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON WEST POINT
681 HARDEE PLACE
WEST POINT, NY 10996-1514

REPLY TO
ATTENTION OF:

IMML-ZA

11 July 2016

U.S. ARMY GARRISON WEST POINT POLICY #21

SUBJECT: Protecting Personally Identifiable Information (PII) and PII Breach Notification Policy

1. REFERENCES:

a. Federal Register, Department of Defense (DoD), dated 1 July 2011, Subject: 32 CFR Part 505, Army Privacy Act Program, Document in Context, Title 32-National Defense, Subtitle A-Department of Defense, Chapter V-Department of the Army, Subchapter A-Aid of Civil Authorities and Public Relations, Part 505-Army Privacy Act Program, PDF. https://www.gpo.gov/fdsys/granule/CFR-2011-title32-vol3/CFR-2011-title32-vol3-part505/content-detail.html

b. Department of Justice, dated 17 July 2015, Subject: Privacy Act of 1974, http://www.justice.gov/opcl/privacy-act-1974

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

d. Department of Defense Directive (DoDD), DoD Privacy Program 5400.11, dated 29 October 2014, http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf

e. Department of Defense (DoD) Memorandum, dated 18 August 2006, Subject: DoD Guidance on Protecting Personally Identifiable Information (PII), http://dpclo.defense.gov/Portals/49/Documents/Privacy/DODGuidancePII.pdf

f. Records Management and Declassification Agency (RMDA), dated 4 September 2015, Subject: Personally Identifiable Information (PII) Breaches, Privacy: Report a PII Incident, Privacy Act through the Privacy Act Tracking System (PATS), http://www.rmda.army.mil/privacy/RMDA-PO-Programs-Privacy-Program.html

g. Department of Defense, DoD Freedom of Information Act Program 5400.7-R, dated September 1998, http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf

h. Information Security Program, DoD 5200.1-R, dated February 2012, http://fas.org/irp/doddir/dod/5200-1r.pdf

i. The Freedom of Information Act, Title 5 USC 552a, dated 23 December 2002.

j. Department of the Army Freedom of Information Act Program, AR 25-55, dated 1 November 1997, http://www.apd.army.mil/pdffiles/r25_55.pdf

k. Information Management and Army Information Technology, AR 25-1, dated 25 June 2013, http://www.apd.army.mil/pdffiles/r25_1.pdf

l. The Army Privacy Program, AR 340-21, dated 5 July 1985, https://www.apd.army.mil/pdffiles/r340_21.pdf

m. The Army Records Information Management System (ARIMS), AR 25-400-2, dated 2 October 2007, http://www.apd.army.mil/pdffiles/r25_400_2.pdf

2. PURPOSE. This memorandum establishes U.S. Army Garrison West Point (USAG WP) policy regarding the protection of PII. PII is any information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information, which is linked or linkable to a specified individual. Note that this does not include the Electronic Data Interchange Personal Identifier (EDIPI), which is public. This information can be in hard copy (paper) or electronic format, stored on desktop computers, laptops, and personal electronic devices, such as blackberries, and found within databases. Managers and administrative personnel in possession of employee personal information must not disclose any personal information except with the consent of the individual or as otherwise authorized by applicable laws or regulations.

3. APPLICABILITY. This policy applies to all employees assigned to the USAG WP.

4. POLICY. It is USAG WP policy that:

a. Any personal information contained in a system of record shall be protected so that the security and confidentiality of the information shall be preserved. 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 current and former Civilian, Military, and Contractor personnel and to protect against any compromise, which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual whom information is stored or transferred in both hard copy and electronic form.

c. For this policy, suspected loss, loss, or compromise of PII will be referred to as a breach. A breach incident occurs when it is suspected or confirmed that PII data in electronic or physical form is lost, stolen, or otherwise made available to individuals without a duty-related official need to know and should be reported through RMDA, Privacy, Report a PII Incident, PATS.

d. 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 take appropriate action upon discovering a breach or failure to take the required steps to prevent a breach from occurring.

5. RESPONSIBILITIES.

a. The Garrison Commander or his designee will:

(1) Notify affected individuals within the Garrison as soon as possible, but no later than ten days after the breach is discovered and the identities of the individuals compromised ascertained. The ten-day period begins after the Garrison is able to determine the identities of the individuals whose PII was compromised in a breach.

(2) Notifications shall be made in writing and sent via US Postal Services, first-class mail with a return receipt, or will be hand delivered to affected personnel and will include a brief description of what happened, date(s) of occurrence and discovery; a description of types of personal information involved; a statement of whether the information was encrypted or protected by other means; steps individuals should take to protect themselves from potential harm; what the command is doing to investigate the breach, to mitigate losses, and to protect against further breaches. All notification information will comply with the guidance (see reference c), DoD 5400.11-R.

b. The Directorate of Human Resources (DHR)/Administrative Services Division (ASD) will:

(1) Be the proponent for this PII policy and serve as the Primary Officer (PO) and designate an Alternate PO.

(2) The PO will be responsible for the management oversight of the Garrison wide implementation of the Privacy Act (PA) program in accordance with 5 USC Section 552a and Public Law 106-554.

(3) Serve as the central Garrison POC for all PII related breached to include but are not limited to:

(a) Assess suspected breach or breach for PII or other issue.

(b) Advise Garrison Commander on mitigation strategy.

(c) Begin data and facts collection to report to Garrison Commander and others as required.

(d) Report the suspected or actual loss to United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery at: http://www.us-cert.gov If computer access is not available, PII incidents can be reported to a 24/7 toll free number at 1-866-606-9580 from the Office of the Administrative Assistant to the Secretary of the Army or US-CERT at 703-235-5110.

(e) Notify Army leadership that an initial report has been submitted to: http://www.rmda.army.mil/privacy/foia-incidentreport.asp_ This email should include US-CERT number and a brief synopsis and contact information for the incident.

(f) Report the suspected or actual loss to the Army FOIA/PA Office within twenty-four hours of discovery. The reporting format and submission guidelines are located at: http://www.rmda.army.mil/privacy/RMDA-PO-Guidance.html

(g) Prepare a Privacy Impact Assessment (PIA) at: http://www.rmda.army.mil/privacy/RMDA-PO-PIA.html

c. Garrison Activity Directors will:

(1) Appoint, in writing, a PO whose duties will be to ensure the protection of PII within their organization and the duties (see reference 1e). A copy of the appointment letter will be provided to the DHR PO.

(2) Create internal procedures to assist in safeguarding against and responding to the breach of PII.

(3) Create and maintain a log of all your incidents involving PII, what your mitigation strategy is and how/when you closed the incident.

(4) Ensure that compromised PII is immediately reported to the PO or as soon as the breach is discovered.

(5) Ensure that all military, civilian, and contractor personnel complete annual web-based PII training and are adequately instructed in their responsibilities related to PII.

(6) Review requests to remove copies of PII from the workplace for their employees following PO review and recommendation.

(7) Maintain a current roster of your respective division.

(8) Ensure that mobile computing devices or removable electronic media do not store or process High Impact PII without express approval from the Designated Accreditation Authority (DAA).

(9) Ensure that mobile computing devices or removable electronic media that processes or stores High Impact electronic PII records shall be restricted to protected workplaces that satisfy all physical and environmental controls necessary.

(10) Ensure that compromised PII is immediately reported to the PO or Alternate PO as soon as the breach is discovered.

d. Network Enterprise Command West Point will:

(1) Provide technical support and an approved data at rest solution for implementation on Government-owned laptops within Garrison activities.

(2) Provide technical support and recommendations on requests to store encrypted PII on disks, CDs, USB flash drives, memory sticks, flashcards, or any other media after obtaining supervisory approval. 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, Civilian and Contractor personnel will:

(1) Handle Privacy Act data as FOUO:

(a) Mark it when it is created or received as "For Official Use Only - Privacy Act of 1974" or "For Official Use Only - Privacy Act Data."

(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 the individual page of a classified document contains only FOUO information, the page will be marked FOUO at the bottom of the page. PII information transmitted outside the 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 unless the material is encrypted and favorable recommendation from DHR/ASD and supervisory approval is obtained. Government PII should never be stored on personally owned notebooks, desktops, flash drives, etc. Mark CDs and DVDs containing PII records appropriately 'For Official Use Only (FOUO) - Privacy Act Data."

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

(e) Remove DoD Common Access Cards (CAC) from their computer before stepping away from the work area, even for brief periods, to ensure protection of PII.

(f) Store PII as to preclude unauthorized access during non-duty hours. PII should be stored in a locked desk, file cabinet, bookcase, or office that is not accessible during non-duty hours. Transport personal records containing PII with a DA Label 87 "For Official Use Only" cover sheet and hand them to an authorized recipient. This is an official or an employee of a DoD component that has a need for the use of the information contained therein in the performance of their official duties (see reference 1b). Receive supervisory approval to transport PII on a portable device. (Note: A copy of the DA Label 87 may be found at: https://www.apd.army.mil/Forms/formrange_forms.asp?valueAD=Labels CAC access required.

(g) Mail PII with a DA Label 87 "For Official Use Only" 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.

(h) Restrict discussions of PII over telephone lines with other Government agencies to a minimum and for official purposes only, and not within areas where those who do not have an official need to know may overhear it.

(i) Cover all facsimile transmissions containing PII with a DA Label 87 "For Official Use Only" sheet. The recipient will be alerted by e-mail or telephone that a scanned PDF file containing PII is being sent. No scanned PDF will be sent until the sender confirms that the recipient is aware and awaiting the transmission.

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

(k) Ensure that all electronic records or electronic records transmitted on or across the network, containing High or Moderate Impact PII shall be transmitted in an encrypted or protected format. Only individuals with a valid need-to-know should transmit or receive PII in hardcopy or electronic form. Acceptable transmissions methods must be Army approved and include but are not necessarily limited to:

(1) Defense Messaging Service.

(2) DoD and Army information systems, including networks, e-mail, and web servers, that utilize Public Key Infrastructure certificates issued by the DoD/Army and approved external PKIs.

(3) Army Handling and Messaging System. Refrain from posting PII on publicly accessible DoD websites. PII posted on a public website is not protected and could allow identity theft to occur. Government business on the Internet is acceptable provided Secure Socket Layers (SSL) and encryption mechanism are used to protect data transmission. Secure Socket Layers exists if the web address begins with "https".

(l) Dispose of PII records IAW AR 25-400-2, The Army Records Information Management System (ARIMS), 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 the contractor uses of one of the above destruction methods.

(m) Purge hard drives and magnetic media to permanently destroy PII information beyond recognition once the information is no longer required.

(n) Complete annual web-based mandatory training requirements on PII and PII Protection Training, link is as follows: https://ia.signal.army.mil/a/pii_module/pii_module/launchpage.htm Provide a copy of completion certificate to their respective training coordinator and Privacy Officer.

(o) Report compromised PII immediately to their supervisor and the Garrison PO or Assistant PO at (845) 938-2964 or by email at: foia/pa@usma.edu

6. Questions regarding this policy may be directed to the Director, Human Resources at (845) 938-8458.

ANDREW S. HANSON
COL, SF
Commanding