- Additional training is also available on the RMDA Website at https://www.rmda.army.mil/privacy/RMDA-PO-Guidance.html.
- Army personnel who mishandle PII are required to take refresher training.

PII Breach Reporting
- Contact your privacy coordinator or supervisor as soon as you suspect or have an actual loss or compromise of PII.
- Report all incidents involving actual or suspected breaches/compromises of PII to http://www.us-cert.gov within one hour of discovery.
- Report all incidents involving actual or suspected breaches/compromises of PII to the HQ Army Privacy Office within 24 hours of discovery at https://www.foia.army.mil/PATS/.
- If your PII is compromised, monitor financial accounts for suspicious activity.
- If your identity is stolen, immediately visit the Federal Trade Commission website for more information and recommended actions http://www.ftc.gov or call 1-877-IDTHEFT.

Social Media
- Assume all information shared on social media sites could be made public.
- Do not post or discuss work related information, especially sensitive/classified information.
- Use privacy settings and controls to limit access to all PII (i.e., creating a folder on AKO that stores PII).

PII Facts
- The majority of PII breaches are due to human error.
- SSNs are the most valuable commodity to an identity thief.
- Insider threat continues to grow, risk is greatest when PII is stolen by a hacker or thief.

FOR MORE INFORMATION
Email: usarmy.belvoir.hqda-oaa-aha.mbx.rmda-foia-privacy-alert@mail.mil
Visit the web at: https://www.rmda.army.mil/privacy/RMDA-PO-Division.html
**Protective Measures**

**Protective Measures**

SSN Reduction-DoDI 1000.30 1 August 2012 Reduc-
tion of Social Security Number (SSN) Use Within DoD.

Limit the use of the SSN, in any form (including the
last four digits), substituting the DoD ID number or
other unique identifier whenever possible.

- Continued collection of the SSN must meet one of
  the acceptable use criteria and be formally justified
  in writing.
- Never include the SSN in a personnel roster.
- Use only officially issued forms. Those that collect
  PII should also have a Privacy Act Statement (PAS).
- The SSN must not be posted on any public facing
  websites.

**IT Equipment**

- Keep your laptop in a secure government space or
  secured under lock and key when not in use.
- Laptops and mobile electronic equipment must have
  full disk/Data at Rest (DAR) encryption.
- Mark all Government furnished external drives or
  mobile media containing PII with “FOUO-Privacy
  Sensitive.”
- Do not create, store or transmit PII on IT equipment
  when the information is not encrypted.
- Never store PII on personal devices.
- Do not maintain PII on a public website or electronic
  bulletin board.
- Do not leave your laptop unattended in a car or car
  trunk, even if the car and trunk are locked.
- Do not check your laptop with or in your luggage
  trunk, even if the car and trunk are locked.

**Email**

- E-mail containing PII must be digitally signed and
  encrypted.
- Under no circumstance should PII be transmitted
  from a government server to a private server i.e., .mil
to a .com email address.
- As a best practice, ensure the e-mail subject line con-
tains “FOUO” if the email contains PII.
- Ensure the body of the email containing PII includes
  the following warning: “FOR OFFICIAL USE ONLY.”
- Ensure you are sending the e-mail to the correct re-
cipients and all have an official need to know.
- Ensure you know what your attachment contains
  (i.e., PII) prior to sending. Do not forget to check all
  tabs if the attachment is an Excel spreadsheet.
- Phishing continues to be on the rise. Ensure you only
  open and respond to legitimate e-mails.

**Faxing**

- Facsimile transmission of PII is prohibited except:
  - When another more secure means is not practical.
  - When a non-Army process requires faxing.
  - When required by operational necessity.
  - When Faxing Internal Government Operations PII
    (i.e., office phone, office email, badge number, etc.).

**Scanning**

- Scanned documents containing PII shall be transmit-
ted using a secure means.
- The network attached MFD “Scan to file” or “scan
to network share” functionality may be used only if
  the sender can verify that all users are authorized
  to have access to the scanned file or network share
  location.

**Electronic Storage Media**

All Internal and removable electronic storage media
must be properly marked and secured. The devices
include, but are not limited to: laptops, printers, copi-
ers, scanners, multi-function devices, hand held de-
vices, CD’s/DVDs, removable and external hard drives,
and flash-based storage media. Classified electronic
storage devices must be physically destroyed.

**Network Shared Drives**

(AR 25-2, Information Management Information As-
surance)

- For files/folders containing PII, ensure that controls
  are in place restricting access to only those with an
  official need to know.
- Limit storage of PII on shared drives whenever pos-
sible.
- Delete files containing PII in accordance with AR 380-
  5, “Department of the Army Information Security Pro-
  gram.”
- Verify that access controls/permissions are properly
  restored following maintenance.

**Disposal**

(AR 380-5, Department of the Army Information Se-
curity Program.)

- Disposal methods are considered adequate if the re-
cords are rendered unrecognizable or beyond recon-
struction (e.g., tearing, burning, melting, chemical
decomposition, burying, pulping, pulverizing, shred-
ding, or mutilation).
- Do not discard documents containing PII in trash or
  recycle bins.

**Shredding**

- It is highly recommended and considered a best
  practice to use a cross-cut shredder.
- For shredder residue size as a best practice, refer to
  NIST Special Publication 800-88.
- An alternative to purchasing a shredder is to contract
  with a GSA approved shredder service.
- In lieu of shredding, the use of burn bags is the al-
ternate option.

**Training and Compliance**

(https://www.rmda.army.mil/privacy/RMDA-PO-Train-
ing.html)

- All new employees are required to take Information
  Assurance (IA) PII training before allowed access to
  networks.
- All Army personnel, including contractors, must com-
mplete annual IA PII training. Local Privacy Officers
  must maintain record of completion by any method,
i.e, spreadsheet log.
- The mandatory training for Army personnel is avail-
able through the DISA IA Education, Training and