REMEMBER THESE RULES:

- ◊ Do not collect PII without proper official authorization.
- ◊ Do not disseminate PII to other members of the DLA workforce unless you know that the release is authorized and there is an official need to know.
- ◊ Do not place PII on shared drives, e-mail folders, multi-access calendars, or the Intranet (eWorkplace, TMT, etc.) unless it is password protected or encrypted.
- ◊ Ensure access to the information is limited to those officers and employees of DLA who have a need for the record in the performance of their official duties.
- ◊ Never place PII on the Internet.
- ◊ Always encrypt and digitally sign email containing PII.

TRAINING REQUIREMENTS

- ◊ All DLA employees must complete Information Assurance (IA) Awareness Training prior to obtaining access to DLA and/or DoD systems; and annually thereafter.
- ◊ All DLA employees must complete DoD Personally Identifiable Information Training prior to obtaining access to DLA and/or DoD systems; and annually thereafter. Supervisors maintain auditable certificates of training completion.
- ◊ All DLA employees must sign the DLA Privacy Safeguards and Responsibilities Certification.
- ◊ All DLA employees must comply with the DoD Privacy Program "Rules of Conduct."[4]

FOOTNOTES

1. "Need to know" refers to those officers and employees of the agency maintaining the records who have a need for the record in the performance of their duties. *See* 5 U.S.C. 552a(b)(1)
2. DLA Policies and Procedures When Personal Information is Lost, Stolen, or Compromised. *See* http://dlaauth.hq.dla.mil/foia-privacy/Documents/Signed%20Memorandum%20to%20DLA%20Executive%20Board%20regarding%20Policies%20and%20Procedures%20for%20PII%20Breach%20sig%20redacted_Redacted.pdf
3. Communication Tasking Order (CTO) 07-15 Task 1, Digital Signatures and Encryption Implementation (HQ LAN Manager email dated June 5, 2008)
4. DoD 5400.11-R, "DoD Privacy Program," at http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf

FOR MORE INFORMATION

Defense Logistics Agency
FOIA / Privacy Act Office, ATTN: DGA
8725 John J. Kingman Road, Suite 1644
Fort Belvoir, Virginia 22060-6221

COM (703) 767-6194, DSN 427 or
(703) 767-5045, DSN 427

Email: hq-privacy@dla.mil
Visit the web at: http://www.dla.mil/HQ/GeneralCounsel/FOIA.aspx

DEFENSE LOGISTICS AGENCY

USERS GUIDE TO

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Revised March 2017

DEFINITION OF PERSONAL INFORMATION / PII

Information about an individual maintained by DLA, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. Such information is also known as "personally identifiable information (PII)."

IF YOU collect, maintain, use, or disseminate Personally Identifiable Information (PII), it must be required to support a DLA function or program as authorized by law or Executive Order. Whether you are working from your desk at the office or at home teleworking, it is your responsibility to:

- ◊ Ensure that the information entrusted to you in the course of your work is kept secure and protected.
- ◊ Minimize the use of Social Security Number (SSNs) and other PII whenever possible.
- ◊ Keep the information timely, accurate, relevant, and complete to the purpose for which it was collected.
- ◊ Allow only those personnel with a "need to know" access to PII.[1]

PROTECTIVE MEASURES

INFORMATION TECHNOLOGY (IT) EQUIPMENT

- ◊ Never leave your laptop unattended.
- ◊ 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 encryption.
- ◊ Mark all external drives or mobile media using DLA Form 1461, "Privacy Act - Safeguard Label."
- ◊ If encryption is not available, do not create, store, or transmit PII on IT equipment.
- ◊ Ensure PII resides only on government furnished IT equipment. Never store PII on personal devices.
- ◊ Do not maintain PII on a public web site or electronic bulletin board.

EMAIL

- ◊ Email containing PII and email subject to the Privacy Act should be digitally signed and encrypted using DoD approved certificates available at https://dod411.gds.disa.mil.[2]
- ◊ Double check that you have the correct email addresses and all recipients have a "need to know" before sending.
- ◊ Double check your attachment to make sure you have selected the right document.
- ◊ Best business practice is to ensure the email subject line contains "FOUO -- Privacy Sensitive" if the email contains PII, and place in the body of the email the following warning, "This email may contain information subject to the Privacy Act of 1974 and is For Official Use Only. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

PRINTED MATERIALS AND FAX MACHINES

- ◊ Verify printer location prior to sending a document containing PII to the printer, and promptly pick up all copies of the documents as soon as they are printed.
- ◊ Double check the fax number prior to transmitting documents with PII, and ensure someone is standing by on the receiving end of the fax. Do not fax PII to unattended fax machines.
- ◊ Ensure all printed documents with PII are properly marked with "FOUO -- Privacy Sensitive."
- ◊ When deemed appropriate, double wrap PII when sending it through the mail. Seal the material in an envelope, address the envelope to an authorized recipient, mark that envelope "FOUO -- Privacy Sensitive," and then place that sealed envelope in a second sealed, unmarked envelope addressed to the authorized recipient.
- ◊ Use DLA Form 1880, "Privacy Act Cover Sheet" when hand carrying/transporting documents containing PII.

DISPOSAL

- ◊ Dispose of documents containing PII by making them unrecognizable by shredding, pulping, or burning.
- ◊ Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.
- ◊ Documents containing PII may also be placed in a burn bag for destruction.
- ◊ Ensure all hard drives are degaussed, properly marked, and accounted for prior to turn in.
- ◊ Do not discard documents with PII in trash or recycle bins.
- ◊ Destroy DLA records in accordance with the DLA Records Schedule

NETWORK SHARED DRIVES

- ◊ Do not store PII on shared drives without first encrypting or password protecting the file.
- ◊ Make sure that access controls are in place to limit access to files/folders that contain PII to those with a "need to know." Check with the J-6 helpdesk for how to do this.

REPORTING PII INCIDENTS

Immediately notify the **DLA Information Technology Operations Center (ITOC) at 1.877.352.6366** if you suspect or discover that PII has been lost, stolen, or compromised.[3]

WHAT IS IDENTITY THEFT?

- ◊ Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.
- ◊ The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year.
- ◊ If your PII is compromised, monitor financial accounts for suspicious activity. See http://www.consumer.ftc.gov/articles/0155-free-credit-reports
- ◊ If your identity is stolen, immediately contact the FTC for more information. http://www.consumer.ftc.gov/features/feature-0014-identity-theft