

Protective Measures

- * Minimize the collection, use, and retention of PII to what is strictly required in order to accomplish the organization's mission.
- * Identify all PII in your organization and determine whether it is being properly protected.
- * Prohibit removal of IT equipment or other PII from the workplace without supervisor approval. Ensure employees are aware of the protection requirements in TRADOC Supplement 1 to AR 25-2 for IT equipment removed from the workplace.
- * Ensure that IT systems use approved data-at-rest encryption.
- * Train users not to click on links or attachments in e-mails that are not digitally signed (phishing continues to be the top attack vector).
- * Ensure that e-mail containing PII or other sensitive information is encrypted.
- * Do not post PII to a public website or to a government site not authorized for PII.
- * Never store or process PII on a personal device or transmit PII from .mil to .com.
- * Ensure that PII is not discarded in trash or recycle bins. Require destruction by cross-cut shredder, burning, or other approved method. Have someone check for compliance regularly.
- * Restrict access to PII to only those who have an official 'need to know.' In particular, verify access settings on network drives and portals.
- * Ensure that information systems processing or storing PII are accredited to do so.
- * Ensure that employees are trained on proper handling of PII.
- * Use a "Privacy Act Data Cover Sheet" (DD Form 2923) when handling PII.

Protecting PII is a responsibility we all share ...

Additional Requirements

- * Information system owners that collect PII must conduct a Privacy Impact Assessment (PIA) to determine whether the PII under their purview is being adequately protected.
- * Information system owners that collect PII from ten or more members of the public per year must obtain an Office of Management and Budget (OMB) control number.
- * Publish a Privacy Act System of Records Notice (SORN) in the Federal Register for all systems which maintain records that are retrieved by a personal identifier.
- * Provide individuals a Privacy Act Statement when asking them to provide personal information. Indicate (a) authority for collection, (b) purpose for collection, (c) routine uses and disclosure; and (d) whether providing information is voluntary or mandatory and consequences of not providing all of the requested information.
- * The use of Social Security numbers in any form (truncated, masked, partially masked, etc.) must comply with DoD acceptable use policy or be eliminated. Use DoD ID numbers or other unique identifier in place of SSNs whenever possible.
- * PII must only be accessible to those with an official 'need to know.' Just because a person routinely uses personal information to perform their duties does not imply that they have a 'need to know' for the personal information of ALL individuals contained in a system where they have access.
- * All new employees are required to take Information Assurance (IA) PII training before being allowed access to networks.
- * Army personnel who mishandle PII are subject to civil and/or criminal penalties.

and is essential for protecting the safety of our personnel.



Leader's Guide to Protecting PII

(Personally Identifiable Information)



Protecting the Force
by
Protecting PII



What is PII?

Information which can be used to distinguish or trace an individual's identity, such as their name, home address, home phone numbers, social security number, date and place of birth, mother's maiden name, biometric records, other demographic, personnel, medical, or financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information.

Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the safety of our personnel and protect them from identify theft, exposure of their personal information, or blackmail.

References

- * U.S. Army Training and Doctrine Command (TRADOC) Regulation 1-8, Operations Reporting.
- * TRADOC Supplement 1 to AR 25-2, Information Assurance.
- * AR 25-1, Army Information Technology.
- * AR 25-400-2, The Army Records Information Management System (ARIMS).
- * AR 380-5, Department of the Army Information Security Program.
- * Office of Management and Budget Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," 22 May 07.
- * Parts I and IV, of DoD Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 5 Jun 09.
- * DoD 5400.11-R, Department of Defense Privacy Program.
- * DoDD 5400-11, DoD Privacy Program.
- * DoDI 1000.30, Reduction of Social Security Number (SSN) Use Within DoD.

What is a PII Breach?

A PII breach is an actual or possible loss of control, unauthorized disclosure, or unauthorized access to personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected.



Most PII breaches can be prevented:

- * Documents containing PII thrown in the trash or recycling.
- * Government laptop, mobile device, or removable media stolen from a vehicle, hotel room, or personal residence.
- * Government computer compromised because a user clicked on an attachment or a weblink in an unsigned "phishing" message or browsed to a malicious website.
- * Alert roster, family member information, or other PII posted on a publicly-accessible website.
- * Use of home computer to process government data.

In Case of PII Breach

It is critical to report any **suspected** PII breach **immediately** to appropriate authorities per TRADOC Regulation 1-8 (www.tradoc.army.mil/tpubs/). **Do not wait until the breach is confirmed!**

IMMEDIATELY

⇒ Notify your Chain of Command

WITHIN 1 HOUR

⇒ Fill out an incident report with USCERT at <http://www.us-cert.gov> or by their 24/7 hotline: (888) 282-0870.

⇒ E-mail TRADOC Operations Center usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil the completed SIR and DD Form 2959 (with US-CERT number).

WITHIN 24 HOURS

⇒ TRADOC Office of the G-6 will report to HQDA Privacy Office and G-6 usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-foia-privacy-alert@mail.mil

WITHIN 10 DAYS

⇒ When required, the organization that had responsibility to control access to the compromised PII **will** notify affected individuals.

This document is available for download at <http://www.tradoc.army.mil/Publications.asp>

Users are invited to send suggested improvements to the Office of the TRADOC Deputy Chief of Staff, G-6, usarmy.jble.tradoc.mbx.g-6-tradoc-iapm@mail.mil

Current as of: 31 Jul 15