Protective Measures

- **Ensure personnel encrypt email designated as Controlled Unclassified Information (CUI)/PII.**
- Minimize the collection, use, and retention of PII to what is required in order to accomplish the organization's mission and function.
- Identify all PII in your organization and determine whether it is being properly protected.
- Prohibit removal of information technology (IT) equipment and/or records containing PII from the workplace without supervisor approval.
- Ensure personnel are aware of the protection requirements in TRADOC Supplement 1 to AR 25-2, requiring IT equipment removed from the workplace to have approved data-at-rest encryption.
- Train personnel not to click on links or attachments in emails that are not digitally signed (phishing continues to be the top attack vector).
- 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. Verify access/ permission 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 safeguarding/handling of PII.
- Use SF 901 (CUI Coversheet) when handling records with CUI/Privacy Act/PII information.

Protecting PII is everyone's responsibility...

Additional Requirements

- Owners of systems/applications/electronic data collections will complete the DD Form 2930 (Privacy Impact Assessment) and may be required to reference or publish a Privacy Act System of Records Notice (SORN) (when information is retrieved using PII), and/or complete an Office of Management and Budget (OMB) control number approval documents (when information is collected from 10 or more members of the public annually).
- Manage and dispose records containing PII IAW AR 25-400-2, AR 380-5, and DA PAM 25-403.
- Provide individuals a Privacy Act Statement when requesting 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.
- Use DoD ID numbers or other unique identifier in place of social security numbers (SSNs) whenever possible. The use of SSN in any form (truncated, masked, partially masked, etc.) must comply with DoD acceptable use policy or be eliminated.
- PII must only be accessible to those with an official need-to-know. Just because a person routinely uses PII to perform their duties does not imply that they have a blanket need-to-know all the personal information of all the individuals contained in a system where they have access.
- Training: Information Assurance/Cyber Security training completed by all personnel before accessing networks, then annually thereafter. Privacy/Civil Liberties (PCL) training completed by all personnel upon reporting, then annually thereafter. Specialized PCL training will be completed, per AR 25-22.
- 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 Personally Identifiable Information (PII)

Protecting the Force
by
Protecting PII

TRADOC G-6

TRADOC G-6
Records Management Office
(757) 501-6529/6523
usarmy.jble.tradoc.mbx.hq-tradoc-foia@army.mil

What is PII?

- Information which can be used to distinguish or trace an individual's identity (i.e., name, SSN, DOD ID, biometric records), alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, and mother's maiden name.
- PII does not have its own retention period. PII is part of a record or system of records and IAW AR 25-400-2, records have assigned disposition schedules that prescribe how long the record is to be maintained, and when to destroy or transfer/ archive them.

Internal vs External Use

- Records containing PII are made available to DoD personnel wo have a need-to-know in the performance of their duties.
- The need-to-know principle dictates that an authorized holder of record/PII, only share when two conditions are met: **1) the requester has the appropriate position and access, and 2) the requester has a need-to-know the information in order to perform his or her job functions.** When both conditions are met, provide the record/PII.
- Verifying that the requestor has the appropriate position is usually straightforward. You see their badge or know that the communication is coming through channels at the appropriate level.
- Verifying their need-to-know, on the other hand, may require some judgment. If unclear the requestor needs the information, then ask the chain of command to verify.
- Before PII is made available to the public (external third parties), a balancing of the public's right to know compared to an individual's right to privacy is analyzed to determine if the record/PII is released or withheld under the Freedom of Information Act, or other laws and regulations.
- Business card/email signature information is PII used to conduct Government business.
- Designated personnel appointed in "public" positions may have their name and organization information on public facing.

What is a PII Breach?

A PII breach is a suspected or confirmed loss of control, unauthorized disclosure, or unauthorized access to PII, where persons without a need-to-know gain access or potential access for other than authorized purposes. The terms 'breach'/ 'incident' and 'violation' are inter-changeable, there is no reporting difference.

Examples of PII Breaches

- An e-mail containing CUI/FOUO/PII information is inadvertently sent to the wrong person or not encrypted IAW AR 25-1, email services.
- PII intended for internal CUI/FOUO use is published on a public facing website.
- A laptop or mobile device is lost or is stolen.
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or discussing Federal benefits (leave or awards).
- Records containing PII thrown in the trash or recycling.
- Government computer compromised because a user clicked on an attachment or a web-link in an unsigned "phishing" message or browsed a malicious website.
- Alert roster, family member information, or other PII posted on a publicly-accessible web site.
- Use of home computer to process government data.

References

- **OMB-17-12** (Safeguarding Against and Responding to the Breach of Personally Identifiable Information)
- **DoDI 5400.11** (DoD Privacy and Civil Liberties Program)
- **DoD 5400.11-R (**DoD Privacy Program)
- **AR 25-1** (Army Information Technology)
- **AR 25-22** (The Army Privacy and Civil Liberties Program)
- **AR 25-55** (The Department of Army Freedom of Information Act Program)
- **AR 25-400-2** (The Army Records Management Program)
- **AR 360-1** (The Army Public Affairs Program)
- **AR 380-5** (Army Information Security Program)
- **AR 530-1** (Operations Security)
- **DA PAM 25-1-1** (Army Information Technology Implementing Instructions)
- **DA PAM 25-403** (Guide to Record Keeping in the Army)
- **DA PAM 25-2-17** (Incident Reporting)
- **TRADOC Regulation 1-8** (Operations Reporting)
- **TRADOC Supplement 1 to AR 25-2** (Information Assurance)

In Case of PII Breach

It is critical to report any suspected or confirmed PII breach immediately to the chain of command in accordance with (IAW) TRADOC Regulation 1-8 and AR 25-22.

1. **IMMEDIATELY: Notify Chain of Command.**
2. **WITHIN (1 HOUR):**
   Send completed Serious Incident Report via encrypted email to the TRADOC Operations Center at usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil, per TRADOC Regulation 1-8. Organizations will no longer submit US-CERT reports, per AR 25-22.
3. **IAW LOCAL STANDING OPERATING PROCEDURE AND DA PAM 25-2-17:**
   Notify your security manager and submit an Army Enterprise Service Desk (AESD) help desk ticket to report the PII breach at https://snpro.aesd-w.army.mil/sp or worldwide at 866-335-2769.
4. **WITHIN (24 HOURS):**
   The organization will contact the TRADOC Privacy Official to ensure a report is submitted to the Army Privacy Office via PATS at: https://www.privacy.army.mil/PATS/.
5. **WITHIN (10 DAYS):**
   In coordination with the Army and TRADOC Privacy Official, the reporting organization will notify affected individuals.

This document is available for download at the TRADOC Privacy Act/PII web site http://www.tradoc.army.mil/PrivacyAct/.

Suggested improvements may be sent to the TRADOC Office of the Deputy Chief of Staff, G-6, usarmy.jble.tradoc.mbx.tradoc-atim1@army.mil

Current as of 8 Nov 2022