



DEPARTMENT OF THE ARMY  
HEADQUARTERS, UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND  
102 MCNAIR DRIVE  
FORT MONROE, VIRGINIA 23651-1047

REPLY TO  
ATTENTION OF

ATIM-T

SEP 20 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Reporting the Loss of Personally Identifiable Information (PII)

1. References:

a. ALARACT message 167/2007, 251400JUL 07, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.

b. TRADOC Policy Letter 16, 30 May 07, subject: Security of Government-owned or Leased Information Technology (IT) Equipment.

2. This memorandum supersedes HQ TRADOC memorandum, ATIM-T, 1 Dec 06, SAB. PII reporting procedures are updated to include the following:

a. Notification requirement to concurrently notify PII.REPORTING@US.ARMY.MIL and the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of a PII-related incident in accordance with reference 1a.

b. PII incident report review by the TRADOC Public Affairs Office for potential publicity and provide input to TRADOC Deputy Chief of Staff, G-6.

c. A sample PII Incident Report and updated references.

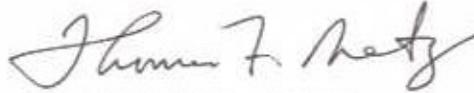
3. The loss of PII continues to be a challenge. Commanders have taken steps to mitigate the loss in accordance with reference 1b, however, in the past 10 months, there were 43 confirmed TRADOC PII incidents reported with a total of 20,376 individuals potentially placed at risk. Forty incidents were the result of stolen laptops. Many of these incidents could have been avoided by diligently protecting and securing IT equipment used to collect PII.

4. TRADOC organizations will continue reporting incidents in which PII is lost, stolen, or compromised, whether in electronic or physical form. Report both suspected and confirmed incidents in accordance with the enclosed TRADOC Reporting Procedures for Loss or Suspected Loss of PII.

ATIM-T

SUBJECT: Reporting the Loss of Personally Identifiable  
Information (PII)

5. Point of contact is Mr. Rick Romero, TRADOC Privacy Program  
Manager, Deputy Chief of Staff, G-6, DSN 680-2237, (757) 788-2237,  
or ricardo.romero@us.army.mil.



Encl

THOMAS F. METZ  
Lieutenant General, U.S. Army  
Deputy Commanding General/  
Chief of Staff

DISTRIBUTION:

Commander  
U.S. Army Accessions Command  
U.S. Army Combined Arms Center  
U.S. Army Combined Arms Support Command  
U.S. Army Maneuver Support Center  
Joint Readiness Training Center Operations Group  
National Training Center Operations Group

Commandants, TRADOC Schools

Director  
Army Capabilities Integration Center  
U.S. Army TRADOC Analysis Center  
U.S. Army Aeronautical Services Agency

Deputy Chiefs of General and Chiefs of Special Staff Offices,  
HQ TRADOC

**TRADOC Reporting Procedures for Loss or Suspected Loss of Personally  
Identifiable Information (PII)**

---

1. References (1a, c, d, and f are located at <https://www.us.army.mil/suite/page/309>):

a. Memorandum, Department of Defense Chief Information Officer, 18 Aug 06, subject: Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII).

b. TRADOC Policy Letter 16, 30 May 07, subject: Security of Government-owned or Leased Information Technology (IT) Equipment (<http://www.tradoc.army.mil/COFS/policyletters.htm>).

c. Memorandum, Deputy Commanding General/Chief of Staff, 31 Oct 06, subject: Guidance on Protecting Data-At-Rest (DAR).

d. ALARACT message 167/2007, 251400JUL 07, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.

e. TRADOC Regulation 1-8, Training and Doctrine Command (TRADOC) Operations Reporting, 7 Jul 06 (<http://www.tradoc.army.mil/tpubs/regs/r1-8.doc>).

f. Memorandum, Office of the Secretary of Defense (OSD), The Deputy Secretary of Defense, OSD 12282-05, 15 Jul 05, subject: Notifying Individuals When Personal Information is Lost, Stolen, or Compromised.

2. Applicability.

a. PII refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., 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, mother's maiden name, etc.

b. For the purpose of this policy, the phrase "loss or suspected loss of PII" or "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized access, or any similar term referring to situations where persons other than authorized users and for any other than authorized purpose have access or potential access to PII, whether physical or electronic. This includes, but is not limited to, posting PII on public-facing web sites; sending via e-mail to unauthorized recipients; providing hard copies to individuals without a need to know; loss of electronic devices storing PII; and use by employees for unofficial business.

c. The procedures outlined below apply to all military and civilian personnel assigned, attached, detailed, or on temporary duty with TRADOC organizations that control or collect PII.

3. Procedures. Commanders will ensure the procedures listed below are followed and delegate execution to the supervisory level required to meet the timeline for reports. Commanders may issue additional requirements to protect PII and report losses/compromises within their chain of command; however, at no time will locally established reporting procedures preclude or replace reporting requirements established herein.

a. Protect PII.

(1) Evaluate all PII under your control for impact of loss or unauthorized disclosure and assign a High or Moderate PII Impact Category according to the definitions established in reference 1a.

(2) Protect electronically stored PII as described in references 1b and 1c. Any sensitive information or PII removed from the workplace must be approved by a supervisor, protected by an Army-approved hard drive encryption solution, and properly labeled.

b. Report PII loss/compromise.

(1) Report all incidents involving lost or compromised PII in electronic or physical form. Report both suspected and confirmed breaches.

(2) Report to US-CERT within 1 hour of discovery as prescribed in references 1a, 1d, and 1e. Use the US-CERT web-based reporting system, <https://forms.us-cert.gov/report/>. US-CERT will e-mail the individual submitting the report a receipt confirmation and report number.

(3) At the same time the US-CERT is notified, submit an e-mail notification to PII.REPORTING@US.ARMY.MIL as prescribed in reference 1d. This e-mail will include the following information: organization involved, date of incident and number of personnel potentially impacted, brief synopsis, and point of contact information. The purpose of this e-mail is to notify Army leadership that an initial report has been submitted to US-CERT.

(4) The notifications in paragraphs (2) and (3), above, are sent directly to the Department of the Army and the Department of Homeland Security; TRADOC does not see these notifications. Therefore, consider all incidents involving lost or compromised PII as an Operational Report (OPREP) reportable incident and include the PII Incident Report with the OPREP in accordance with reference 1e. The PII Incident Report is available via the TRADOC homepage (<http://www.tradoc.army.mil/tpubs/TRADOCforms.htm>). See Enclosure 1 for a sample PII Incident Report. The PII Incident Report provides visibility to HQ TRADOC leaders and is

intended to initially capture the same information submitted in paragraphs (2) and (3), above.

(5) Notify affected individuals as soon as possible, but not later than 10 days after the loss or compromise of PII is discovered, in accordance with reference 1f. Coordinate with local Staff Judge Advocate prior to sending the notification letter. See Enclosure 2 for a sample letter. At a minimum, advise the individuals of the following:

- (a) Specific data involved.
- (b) Circumstances surrounding the loss, theft, or compromise.
- (c) A statement as to whether the information was protected.
- (d) Protective actions the individual can take.

c. The TRADOC Emergency Operations Center (EOC) will apply procedures established in reference 1e to report incidents of lost/compromised PII. PII incidents are reportable to the ARMYWATCH/Army Operations Center (AOC). The EOC will transmit the OPREP with attached PII Incident Report to the ARMYWATCH/AOC and TRADOC Deputy Chief of Staff, G-6.

d. The TRADOC Deputy Chief of Staff, G-6 designated representative will review all TRADOC PII Reports submitted for severity and potential consequences of the incident.

(1) Provide the TRADOC EOCWATCH an after normal duty hour on-call POC roster to address issues that may arise.

(2) Follow up with the DA Privacy Office to ensure receipt of the PII Incident Report and complete follow-up coordination as needed.

(3) Coordinate and provide the HQ TRADOC leadership and staff, HQDA, and other organizations follow-up reports/updates to initial OPREP, as necessary, regarding the incident and related matters.

(4) Coordinate with other organizations as necessary and prepare the TRADOC-level response.

e. TRADOC Public Affairs designated representative will determine the potential for publicity and the potential consequences of that publicity, and provide input to TRADOC Deputy Chief of Staff, G-6.

4. This policy is effective immediately.

2 Enclosures

- 1. Sample PII Incident Report
- 2. Sample Notification Letter

-SAMPLE-

TRADOC PERSONALLY IDENTIFIABLE INFORMATION (PII) INCIDENT REPORT <small>(blocks marked with * indicate required items for United States Computer Emergency Readiness Team (US-CERT) on-line Report)</small>		
<b>IMPACT CATEGORY</b>		
<input type="checkbox"/> High Impact (> or = 500 individual PII on the system)	Actual number of PII <input type="text"/>	
<input checked="" type="checkbox"/> Medium Impact (< 500 individual PII on the system)	OR	
<input type="checkbox"/> Unknown Impact	Estimated number of PII <input type="text" value="99"/>	
<b>REPORTING ORGANIZATION</b>		
1. ORGANIZATION xxxx Recruiting Station, Lansing, MI - USAREC	2. POINT OF CONTACT NAME/ TELEPHONE/ EMAIL: CPT John Smith/ 517-111-1111/ cptjohn.smith@us.army.mil	
3. DATE/ TIME REPORTED TO US-CERT (include tracking number): 5 Sep 07/ 1400 (USCERT06822)	4. * INDIVIDUAL REPORTING TO US-CERT (Name/Email/ Contact Number) SFC John Smith/ 517-111-1111/ stjoh.smith@us.army.mil	
<b>INCIDENT INFORMATION</b>		
5. TYPE OF REPORT: <input checked="" type="checkbox"/> Initial <input type="checkbox"/> Follow-up <input type="checkbox"/> Final	6. * DATE/TIME INCIDENT OCCURRED (local time)    * Time Zone 5 Sep 07/ 1200-1300    CST	
7. WAS THE DATA ENCRYPTED? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If data was encrypted, what Data-at-Rest solution was implemented? POINTSEC		
8. * LAW ENFORCEMENT NOTIFICATIONS MADE (Civilian and Military)(Agency names and case numbers): Lansing Police Department - case number LPD 174-2007		
9. PROVIDE SHORT DESCRIPTION OF THE INCIDENT AND POTENTIAL IMPACT THE LOSS OF PII WILL HAVE ON THE COMMAND: Brief description of incident, type of information lost and notifications either made or will make to individual(s) whose information was compromised:  Active duty recruiter secured an assigned government laptop with a cable lock to an immobile object in the recruiting station and went to lunch at a local nearby establishment. Upon return, it was discovered that the recruiting station front door window was smashed and the cable lock had been cut by person(s) unknown with an unknown device. The laptop contained personally identifiable information for approximately 99 civilian potential recruits consisting of name, social security number, home address, and home telephone number. Replication of the last hard drive image will be conducted in order to obtain a better determination of affected individuals so they can be notified of the incident and provided additional information to assist the affected members in understanding the potential risks and precautions they can take to protect their identities. Local police were immediately notified. United States Computer Emergency Readiness Team (US-CERT) was notified at the lowest level possible in order to meet the one-hour reporting requirement via their web based reporting system. Immediately after notifying US-CERT, an email was sent to pii.reporting@us.army.mil providing a brief synopsis and point of contact information. The potential impact is minimized as the laptop and the data contained on the laptop was encrypted with an Army-approved data at rest solution. Investigation continues by local police.		
10. * OPERATING SYSTEM (OS) OF AFFECTED COMPUTER(S):	XP	
11. * ADDITIONAL OS AND PATCH INFORMATION (if not know enter "Unknown"):	Unknown	
12. * LOCATION OF SYSTEM AFFECTED (City/State):	Lansing, MI	
13. * INCIDENT CATEGORY TYPE:		
<input type="checkbox"/> CAT 0 - Exercise/ Network Defense Testing	<input type="checkbox"/> CAT 1 - Unauthorized Access	<input type="checkbox"/> CAT 2 - Denial of Service
<input type="checkbox"/> CAT 3 - Malicious Code	<input type="checkbox"/> CAT 4 - Improper Usage	<input type="checkbox"/> CAT 5 - Attempted Access
<input checked="" type="checkbox"/> CAT 6 - Under Investigation		
14. OTHER NOTIFICATIONS COMPLETED: (list date/time, organization and title of Individual) (i.e. 1530hrs, 4 Nov 06, USACC Commander and PAO): USAAC Command Operations Center was notified at 0900hrs, 5 Sep 07; USAAC Command was notified at 0930hrs; USAAC Public Affairs Officer was notified at 1000hrs		
15. ACTIONS TAKEN BY THE COMMAND/ REMARKS (i.e. PIA conducted, letters of notification completed on 4 Nov 06, PAO issued statements, etc): Letters of notification will be sent out NLT than 10 days.		

TRADOC PII INCIDENT REPORT (FEB 2007)

-SAMPLE-

Encl 1 to Encl



REPLY TO  
ATTENTION OF:

[Office]

DEPARTMENT OF THE ARMY

Organization  
Street Address,  
City, State

[DATE]

Name  
Street Address  
Apartment 3  
Anywhere, NY 00000-0000

Dear [Name]:

The purpose of this letter is to inform you that on [DATE] a [identify information system] containing your personal information provided to the [ORGANIZATION] was [stolen]/[lost]. The specific data involved was [data]. The circumstance surrounding the [theft] [loss] [explain circumstances].

Your personal information is protected by internal security measures. We provide you with this notice to ensure you take the necessary precautions to monitor your affairs.

Social Security Administration has a toll-free number 1-800-772-1213, or additional contact information is found on their web site <http://www.ssa.gov/reach.htm>.

You may also want to monitor your credit reports by contacting:

1. Transunion <http://www.transunion.com/index.jsp>
2. Equifax <http://www.equifax.com/>
3. Experian <http://www.experian.com/>

For information on Identity Theft, visit <http://www.ftc.gov/>.

The above listed actions are not an exhaustive list of protective measures you may choose to take. There may be additional organizations or people with whom you may wish to consult, depending on your circumstances.

Should you have any questions, please contact [provide point of contact].

Sincerely,

[signature block]

Encl 2 to Encl