DEPARTMENT OF THE ARMY
U.S. ARMY CORPS OF ENGINEERS
441 G STREET NW
WASHINGTON, D.C. 20314-1000

FEB 2 2 2007

CECI-A (25-1a2)

MEMORANDUM FOR Commanders, Major Subordinate Commands, Field Operating Activities and Laboratories

SUBJECT: Protecting Personally Identifiable Information (PII)

1. Recent events involving the possible compromise of U.S. Army Corps of Engineers (USACE) employee's personal information have underscored the importance of protecting that information. All USACE personnel have the responsibility to ensure that personally identifiable information (PII)[1] of current and former DoD, Army and USACE civilian, military, and contractor personnel is safeguarded.

2. References (see enclosure).

3. To safeguard PII and comply with new Office of Management and Budget (OMB), DoD and Army requirements, all Commands will take a more active role in monitoring the use of personally identifiable information and reporting its loss, theft or compromise. Specifically, Commands will:

a. Ensure all personnel are aware of their responsibilities for safeguarding personally identifiable information in all media and format, the rules for acquiring and using such information, the rules for reporting a loss, theft or compromise, and the penalties for violating these rules.

b. Ensure that there are adequate safeguards to prevent the loss, theft, compromise or unauthorized access to personally identifiable information. Personally identifiable information will not be made available to an individual or entity outside of USACE, except pursuant to a properly processed Privacy Act (PA) or Freedom of Information Act (FOIA) response. The information will not be placed on websites, file transfer protocol (FTP) sites or information systems that are readily accessible to the public.

---

[1] Personally Identifiable Information (PII) is defined as any information about an individual maintained by an agency, 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, OMB M-06-19, 12 July 2006 and DoD Guidance on Protecting PII, 18 Aug 2006.

c. Ensure all personnel are aware of the reporting requirements and accomplish them as incidents occur.

4. When a Command discovers the potential loss, theft, compromise or unauthorized access to personally identifiable information, it will:

a. Report that security incident within one (1) hour of discovery to the local USACE Information Assurance Security Officer (IASO). The IASO will provide the reporting Command with additional instructions for reporting, investigating and remediating the incident at that time.

b. Submit a PII Security Incident Report within 24 hours of the initial discovery to the USACE Privacy Act Officer. POC is Linda C. Genovese, USACE Privacy Act Officer, e-mail Linda.C.Genovese@usace.army.mil, telephone 202-761-7138.

c. Notify impacted individuals within 10 days of discovery of the incident, including what remedial actions have been and/or will be taken and what protective actions the individual can take. Notifications will be coordinated with the local Office of Counsel.

5. The USACE Corporate Information Directorate (CECI) will process the PII Security Reports and:

a. Submit a PII Security Incident Report to the United States Computer Emergency Readiness Team (US-CERT), a Department of Homeland Security reporting tool, within one (1) hour of discovery by the responsible Command. POC is Joy L. Renfro, USACE Information Assurance Program Manager, CECI, e-mail Joy.L.Renfro@usace.army.mil, telephone 601-634-2639.

b. Submit a PII Security Incident Report to the Department of the Army FOIA/PA Office within 24 hours of discovery. Army will forward the report to the DoD Privacy Office within 48 hours. POC is Linda C. Genovese, USACE Privacy Act Officer, CECI, e-mail Linda.C.Genovese@usace.army.mil, telephone 202-761-7138.

6. The points of contact for this memorandum are Ms. Joy L. Renfro and Ms. Linda C. Genovese.

Encl

CARL A. STROCK
Lieutenant General, USA
Commanding

SUBJECT: Protecting Personally Identifiable Information (PII)
CECI-A (25-1a2)

References.

a. OMB Memorandum, M-06-15, "Safeguarding Personally Identifiable Information," dated 22 May 2006.
b. OMB Memorandum, M-06-16, "Protection of Sensitive Agency Information," dated 23 June 2006.
c. OMB Memorandum, M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," dated 12 July 2006.
d. DoD Memorandum, "Notifying Individuals When Personal Information is Lost, Stolen, or Compromised," dated 15 July 2005.
e. DoD CIO Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," dated 18 August 2006.
f. DEPSECDEF Memorandum, "Information Security/Website Alert," dated 7 August 2006.
g. AR 25-1, Army Knowledge Management and Information Technology, dated 15 July 2005.
h. AR 25-2, Information Assurance, dated 14 November 2003.
i. USACE CECI-IA e-mail, "Awareness of OMB Memo M-06-19/Reporting of Security Incidents," dated 4 August 2006.

Encl