Texas Military Forces
Joint Force Headquarters
Adjutant General's Department
Austin, Texas 78763-5218
1 October 2007

***Joint Force Texas**
(JFTX) Regulation 1-01

Information Management

Safeguarding Personally Identifying Information (PII)

By Order of the Adjutant General:

CHARLES G. RODRIGUEZ
Lieutenant General (TX), TXARNG
Adjutant General

Official:
MELISSA C. HARDEN
CW2, AG, TXARNG
J5 – Policy Branch

Summary. This regulation provides policy and guidance for the safeguarding of Personally Identifying Information (PII), such as Social Security Numbers (SSNs), to minimize the risk of identity theft and fraud.

Applicability. This regulation applies to all elements and personnel of the Texas Military Forces.

Internal Control Systems. This regulation is subject to the requirements of AR 11-2, but does not contain control measures.

Suggested Improvements. The proponent of this regulation is the Director of Personnel – J1. Users are invited to send comments and suggested improvements to The Adjutant General of Texas, (JFTX-J1), P.O. Box 5218, Austin, Texas 78763-5218.

Distribution. A

Contents

Appendices

1. **Purpose.** Establish policy and provide guidance for all TXMF personnel regarding the safeguarding of PII, such as Social Security Numbers (SSNs), to minimize the risk of identity theft and fraud.

2. **Eliminating the unnecessary use of SSNs as a personal identifier.**

a. In accordance with the references listed at Appendix C, unnecessary printing and displaying of the SSN on forms, reports, and computer display screens will be eliminated.

b. When the use of the full SSN is required, access must be restricted to only those individuals whose official duty requires such access.

c. When the SSN is required for personal identification, limit to the last four digits unless the full SSN is required.

3. **Transmittal of media containing PII.**

a. Internally. Exercise caution before transmitting personal information over e-mail to ensure it is adequately safeguarded. When sending employee's sensitive and personal information over email, ensure:

(1) there is an official need;

(2) all addressee(s) are authorized to receive it under the Privacy Act; and

(3) it is protected from unauthorized disclosure, loss, or alteration.

b. Outside Agencies.

(1) Do not disclose personal information to anyone outside the TXMF unless specifically authorized by the Public Information Act and the Privacy Act. Such information is disclosed only as compatible with the purpose for which the information was originally gathered or when written permission of the user has been obtained.

(2) If authorized to release information involving TXMF personnel, the SSN (along with the home address and home telephone number) must be redacted. That is, it must be edited to protect confidential information.

4. All information storage devices with PII must be marked with a "For Official Use Only (FOUO) - Privacy Act Data" label and safeguarded against theft and unauthorized use.

5. Personnel having knowledge of loss or compromise of PII will report through chain of command according to the following:

a. Unauthorized use or transmittal of PII. Report compromise of PII with all known information as an incident report to the owning directorate or MACOM.

b. Theft or loss of equipment containing PII.

(1) Report incident to the Provost Marshall, 512-782-6743 or to local law enforcement if loss occurs off a military reservation.

(2) Report compromise of PII with all known data loss to the owning directorate or MACOM.

c. The directorate or MACOM responsible will report the incident to the Joint Operations Center (JOC), take immediate actions to contain loss, and investigate the incident, providing assistance and information to the JOC.

d. The JOC will coordinate the response, including notification of personnel potentially affected and coordination with Public Affairs Office (PAO) for Adjutant General's Department (AGD) response. If an electronic breach occurred, the JOC or, if appropriate, the J6, will notify The United States Computer Emergency Readiness Team within 1 hour. Reports can be made via the following link: https://forms.us-cert.gov/report/ The TXMF Freedom of Information Act/Privacy Act Officer must be notified within 24 hours, 512-782-5443.

e. Personnel at risk shall be advised to review credit card statements and credit reports regularly, and if suspected identity theft occurs, should contact the financial institution involved, file a police report to local authorities, and file a complaint with the Federal Trade Commission. The Texas State Attorney General's Office also provides an Identity Theft Victim's Kit, which includes all necessary advice.

6. **Training.** All personnel authorized to access PII must understand their responsibility to protect sensitive and personal information. JFTX-J6 will make training available to all users of the TXMF network annually. This training meets physical and information security training requirements of this regulation."

a. Annual training and educational programs which include Privacy Act and Freedom of Information Act requirements, will reinforce awareness of employee responsibilities. Documentation of training will be maintained by next level supervisors, commanders, or managers.

b. All individuals authorized to access PII must be familiar with proper labeling, storage and disposal of material containing PII in accordance with 5 C.F.R., part 293, AR 340-21, Air Force Instruction 33-332, and this regulation.

c. All individuals authorized to access PII must be familiar with incident reporting requirements in case of loss or compromise of PII in accordance with this regulation.

7. **Disposal.** Disposal of all paper-based collection tools must be in accordance with the General Record Schedule issued by the National Archives and Records Administration.

8. **Component/Directorate/MACOM responsibilities.**

a. Review their current procedures to ensure compliance with this regulation.

b. Assign a Privacy Official for oversight and advice on matters of Privacy in accordance with component regulations. Notify TXMF FOIA/PA POC.

c. Report PII-related incidents to the Joint Operations Center (JOC), take immediate actions to contain loss, and investigate the incident, providing assistance and information to the JOC.

Appendix A

Sample Notification Considerations

For distribution to personnel potentially affected by PII loss:

1 - I'm a Guard member, how can I tell if my information was compromised?

At this point there is no evidence that any missing data has been used illegally. However, the Texas Military Forces (TXMF) is asking all members to be extra vigilant and to carefully monitor their bank statements, credit card statements and other statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved, contact law enforcement, and contact the Federal Trade Commission for further guidance.

2 - What is the earliest date at which suspicious activity might have occurred due to this data breach?

The information was stolen (compromised) from (by) a member of the (TXANG, TXARNG, TXSG) the month of August, 2007 (when). If someone has misused or committed fraud or identity theft crimes with this information, it is likely that member may notice suspicious activity during the month of August or September 2007.

3 - I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

The TXMF strongly recommends that members and employees closely monitor their financial statements and visit the TX Attorney General's Department website at http://www.oag.state.tx.us to obtain the Identify Theft Victim's Kit for more recommendations.

4 - Should I reach out to my financial institutions or will the TXMF do this for me?

The TXMF does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious or illegal activity.

5 - Where should I report suspicious or unusual activity?

The Federal Trade Commission (FTC) recommends the following four steps if you detect suspicious activity:

Step 1 - Contact the fraud department of *one* of the three major credit bureaus:

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241;
Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013
TransUnion: 1-800-680-7289; www. transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Step 2 - Close any accounts that have been tampered with or opened fraudulently.

Step 3 - File a police report with your local police or the police in the community where the identity theft took place.

Step 4 - File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by telephone: 1-877-438-4338, online at www.consumer.gov/idtheft, or by mail at Identity Theft Clearinghouse, Federal Trade Commission (FTC), 600 Pennsylvania Avenue, NW, Washington DC 20580.

6 - I know the TXMF maintains my health records; was this information also compromised?

No (Yes) electronic medical records were (not) compromised. The data lost is primarily limited to an (individual's name, address, date of birth, and social security number.) However, this information could still be of potential use to identity thieves and we recommend that all members be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7 - What is the TXMF doing to ensure that this does not happen again?

The TXMF is working with law enforcement and others to investigate this data breach and to develop safeguards against future incidents in accordance with current TXMF PII Regulation.

8 - Where can I get further, up-to-date information?

The AGD website will feature up-to-date news and information. More information will be posted at http://www.agd.state.tx.us when it becomes available.

Appendix B

Sample FOUO Statement

FOR OFFICIAL USE ONLY (FOUO) - Privacy Act Data
The information contained in this e-mail and any accompanying attachments may contain sensitive information, which is protected from mandatory disclosure under the Freedom of Information Act (FOIA), 5 USC 522. It should not be released to unauthorized persons. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking any action in reliance on this information is prohibited. If you received this e-mail in error, please notify me immediately by phone or return e-mail.

Appendix C

References

5 U.S.C. § 552a, The Privacy Act of 1974, 31 December 1974.

5 C.F.R., Part 293, Personnel Records, Basic Policies on Maintenance of Personnel Records, Office of Personnel Management, 1 January 2001.

§ 552. 117 and § 552.021, The Texas Public Information Act, 4 May 1993.

DoD 5400.11-R, DoD Privacy Program, Office of Director, Administration and Management, dated 14 May 2007.

DoD 5400.7-R, DoD Freedom of Information Act Program, Directorate of Freedom of Information and Security Review, dated September 1998.

AR 340-21, Army Privacy Program, 22 June 2004.

AFI 33-332, Privacy Act Program: Communications and Information, 29 January 2004.

Memorandum For Chief Human Capital Officers, Office of Personnel Management, Subject: Guidance on Protecting Federal Employee Social Security Numbers and Combating Identify Theft, 18 June 2007.

Memorandum, JFTX P07-13, Texas Military Forces Policy for Release of Information, dated 1 August 2007.

Appendix D

GLOSSARY

Section I
Abbreviations

AFI
Air Force Instruction

AGD
Adjutant General's Department

AR
Army Regulation

C.F.R.
Code of Federal Regulations

DOD
Department of Defense

FOIA
Freedom of Information Act

FOUO
For Official Use Only

FTC
Federal Trade Commission

IAW
In Accordance With

JFTX
Joint Force Texas

JOC
Joint Operations Center

MACOM
Major Command

PAO
Public Affairs Office

PII
Personally Identifying Information

SSN
Social Security Number

PIA
Public Information Act

TXANG
Texas Air National Guard

TXARNG
Texas Army National Guard

TXSG
Texas State Guard

TXMF
Texas Military Forces

U.S.C.
United States Code

UNCLASSIFIED

TXMFPD

DATA FILE: C:\Documents and Settings\hardenmc\Desktop\JFHQ REGS
DOCUMENT: JFTX 1-01
SECURITY: UNCLASSIFIED
DOC STATUS: INITIAL PUBLICATION