-----Original Message-----

From: FAMSBroadcastMessage

Sent: Fri 22-Jun-07 14:19

Subject: Protection of Sensitive Data

From TSA's Acting Deputy Assistant Secretary

TSA is committed to ensuring that all sensitive data collected and maintained by the agency is secure and used properly. In support of this effort, TSA has formed the Information Protection Commission to conduct a comprehensive review of TSA's information protection policies and practices.

We want to ensure that we have the right procedures in place to safeguard all sensitive data we use every day.

What are the responsibilities of all TSA employees?

ALL employees are responsible for safeguarding sensitive data. Every employee should know the type and location of all Sensitive Security Information (SSI) and Sensitive Personally Identifiable Information (PII) under his or her control, in any format, including any SSI or Sensitive PII extracted from a protected document, such as a personnel record or report. Sensitive data includes not only SSI and PII, but other personal and operational data that is not publicly available.

What is SSI and Sensitive PII?

SSI is information related to transportation security activities that, if publicly disclosed, would be detrimental to transportation security. It can only be shared with covered persons with a need to know.

Sensitive PII includes full name plus Social Security numbers, driver's license numbers, dates of birth, financial information (e.g., account numbers and electronic funds transfer information), medical information, account passwords or personal identification numbers (PINs).

Here is a simple list of DOs and DON'Ts to follow:

- DO take information security seriously. If you see an unfamiliar person wandering in an area where sensitive information is used or kept, ask if they need assistance or report it to your supervisor.

- DO store SSI and PII in a locked desk, cabinet or office when not in use.

- **DO always use the SSI header and footer markings for SSI information.**

- DO use the designated SSI disposal bins or destroy sensitive data using an approved method such as cross-cut shredding. Ask for assistance if unsure.

- DON'T release sensitive information without a need to know. If in doubt, ask your supervisor.

- DON'T ever leave SSI and PII unattended or in an open area.

- DON'T take PII outside of TSA facilities except under approved telework arrangements or when approved by a supervisor to perform official TSA duties.

- DO only use TSA issued equipment to store and process sensitive information and maintain positive control of that equipment.

- DO password-protect all SSI and PII stored on TSA-issued external storage media, such as thumb drives or external hard drives.

- DO ensure that TSA-issued laptop computers are encrypted by the TSA Information Technology Division. All laptop computers MUST be attached to the intranet for at least one eight-hour period every two months to ensure that encryption software and other software updates are installed. To confirm that your laptop has encryption software installed and running, please click the following link:

  <https://staffcollaborator.tsa.gov/sites/optcio/it/OpEffect/Credant/SharedDocuments/VerifyGuardianShield.doc

  <https://staffcollaborator.tsa.gov/sites/optcio/it/OpEffect/Credant/Shared%20Documents/Verify%20Guardian%20Shield.doc> >.

To report that your laptop does not have encryption software installed, please click here

<mailto:mscaustintsawp@unisys.com?subject=Credent%20Not%20Installed%20or%20Functioning%20Incorrectly&body=%20Email%20Address:%0D%0A%0D%0A%20Dell%20Asset%20Tag:%0D%0A%0D%0A%20Computer%20Name:%0D%0A%0D%0A%20Phone%20number:> .

- DO lock your computer workstation when you step away.

- DO double check e-mail addresses when sending sensitive information.

- DO use the following footer when emailing any PII in both the email and the attachment: "Warning: Contains information controlled under the Privacy Act of 1974 (5 U.S.C. 552a)."

- **DO use password-protected attachments to e-mail any sensitive information.**

- DON'T ever store sensitive information on personal electronic equipment such as personal thumb drives and personal hard drives.

- DON'T WAIT - ALWAYS immediately report a loss or suspected loss or compromise of sensitive information, including SSI or PII, to your supervisor.

Gale Rossides

Acting Deputy Assistant Secretary