*Attachment 2*

*Training of Employees and Contractors with Access to Personnel-Related Data*

The attached document, *Protecting & Handling Personnel-Related Data – Quick Reference Guide* should be provided to all employees as part of the combined training. This document is also available at www.dhs.gov/privacy under Privacy Reports and Statements.

## Protecting & Handling Personnel-Related Data – Quick Reference Guide

**Do** make sure all personnel-related data is marked "For Official Use Only" or "Privacy Data."

**Do** protect personnel-related data according to the privacy and security safeguarding polices.

**Do** report any unauthorized disclosures of personnel-related data to your supervisor, Program Manager, or Information System Security Manager.

**Do** immediately report any suspected security violation or poor security practices relating to personnel-related data.

**Do** lock up all notes, documents, removable media, laptops, and other material containing personnel-related data when not in use and/or under the control of a person with a need to know.

**Do** log off, turn off, or lock your computer whenever you leave your desk to ensure that no personnel-related data is compromised.

**Do** password protect and as appropriate, encrypt all personnel-related data documents sent via e-mail. Do not include the password in the body of the email containing the attachment.

**Do** destroy all personnel-related data in your possession when no longer needed and continued retention is not required.

**Do** be conscious of your surroundings when discussing personnel-related data. Protect verbal communication with the same heightened awareness as you would paper or electronic personnel-related data.

**Don't** leave personnel-related data unattended. Secure it in a locked drawer, locked file cabinet, or similar locking enclosure, or in a room or area where access is controlled and limited to persons with a need to know.

**Don't** take personnel-related data home, in either paper or electronic format, without written permission of your supervisors, office chief, or Information Security Systems Manager, as required.

**Don't** discuss or entrust personnel-related data to individuals who do not have a need to know.

**Don't** discuss personnel-related data on wireless or cordless phones unless absolutely necessary. Unlike landline phones, these phones can be more easily intercepted.

**Don't** put personnel-related data in the body of an e-mail. It must be password-protected as an attachment.

**Don't** dispose of personnel related data in recycling bins or regular trash unless it has first been shredded.