



To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

REVISION: This directive supersedes TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*, dated March 13, 2008.

SUMMARY OF CHANGES: Definition of sensitive personally identifiable information (PII) is updated to align with DHS *Handbook for Safeguarding Sensitive Personally Identifiable Information*.

1. **PURPOSE:** This directive provides TSA policy and procedures for handling sensitive PII.
2. **SCOPE:** This directive applies to all TSA employees and contractors.
3. **AUTHORITIES:**
 - A. DHS Privacy Act Procedures, 6 C.F.R. §5.31
 - B. DHS Privacy Incident Handling Guidance
 - C. DHS *Handbook for Safeguarding Sensitive Personally Identifiable Information*
 - D. Office of Management and Budget (OMB) Guidance, M-06-15
 - E. OMB Guidance, M-07-16
 - F. Privacy Act of 1974, 5 U.S.C. 552a
4. **DEFINITIONS:**
 - A. **PII:** Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S.
 - B. **Sensitive PII:** Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any grouping of information that contains the individual's name or other unique identifier plus one or more of the following elements:
 - (1) Driver's license number, passport number, or truncated SSN (such as last-4 digits)
 - (2) Date of birth (month, day, and year)

- (3) Citizenship or immigration status
- (4) Financial information such as account numbers or Electronic Funds Transfer information
- (5) Medical information
- (6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PINs)

NOTE: Other PII may be "sensitive" depending upon its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or a public phone directory of agency employees contains PII but is not sensitive.

5. RESPONSIBILITIES:

A. TSA Employees and contractors are responsible for:

- (1) Complying with the Privacy Act, and TSA and DHS privacy policies and procedures;
- (2) Reporting loss, theft, or unauthorized access to sensitive PII within one hour of discovery; and
- (3) Reviewing their responsibilities under this management directive at least annually.

B. Supervisors and managers are responsible for ensuring subordinates review their responsibilities under this directive at least annually.

C. Director, Privacy Policy and Compliance is responsible for:

- (1) Formulating and communicating official TSA privacy policies;
- (2) Monitoring agency compliance with all applicable Federal privacy laws and regulations and implementing corrective, remedial, and preventive actions whenever necessary; and
- (3) Ensuring that personal information contained in Privacy Act systems of records is handled in full compliance with the Privacy Act, 5 U.S.C. 552a, as amended.

D. Chief Information Officer is responsible for issuing or approving desktop and laptop computers, hard drives, thumb drives, or other storage devices.

6. POLICY: TSA employees and contractors must implement special handling procedures for TSA data containing sensitive PII.

7. PROCEDURES: TSA employees and contractors must implement the procedures in the Appendix, *TSA Sensitive PII Handling Requirements*. TSA encryption policy can be found in the [TSA Office of Information Technology Standard](#).

8. EFFECTIVE DATE AND IMPLEMENTATION: This directive is effective immediately upon signature.

APPROVAL

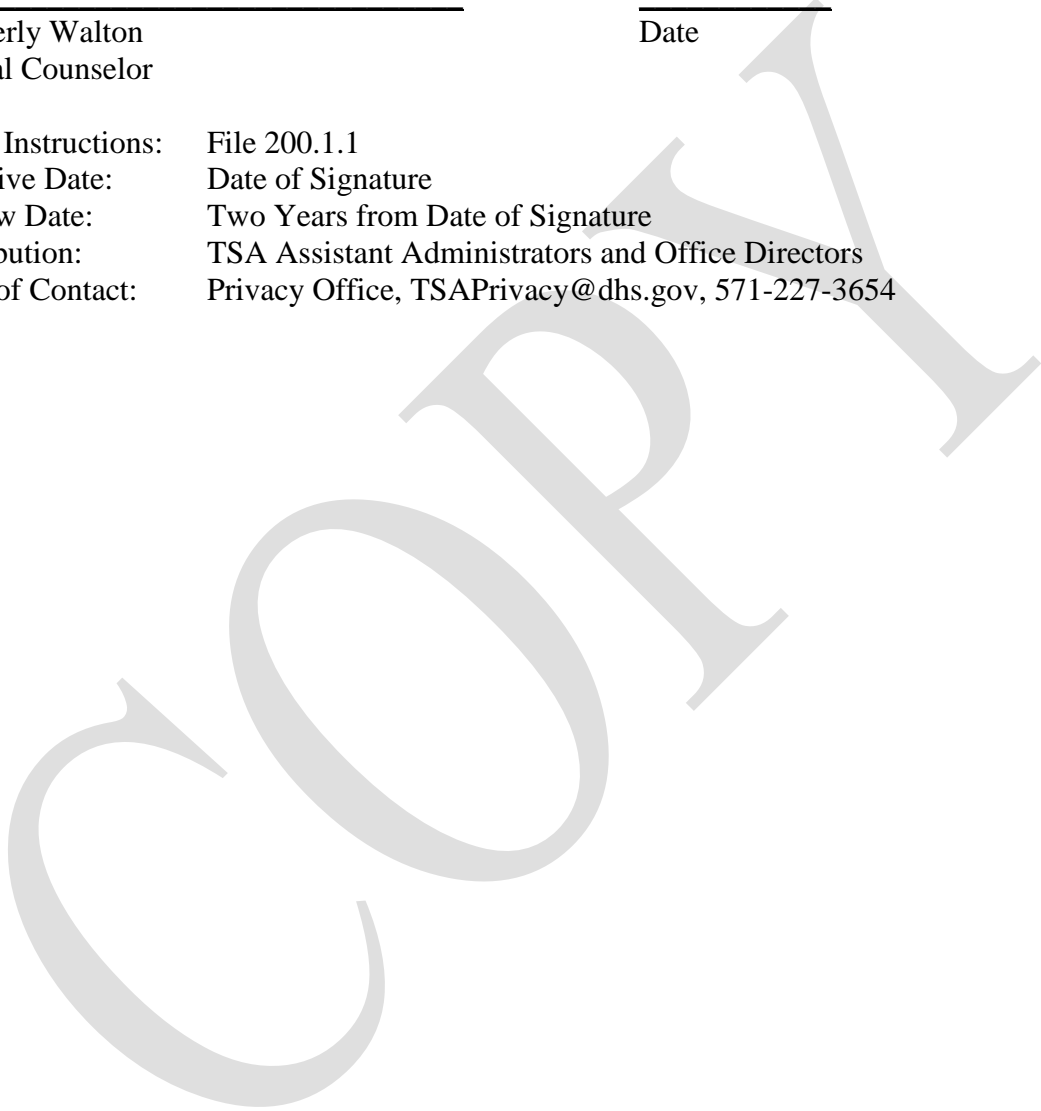
Signed

12/9/2008

Kimberly Walton
Special Counselor

Date

Filing Instructions: File 200.1.1
Effective Date: Date of Signature
Review Date: Two Years from Date of Signature
Distribution: TSA Assistant Administrators and Office Directors
Point of Contact: Privacy Office, TSAPrivacy@dhs.gov, 571-227-3654



Appendix

TSA Sensitive PII Handling Requirements

- A. Physically secure sensitive PII (e.g., drawer, cupboard, safe) when not in use and/or under the control of a person with a need-to-know. Sensitive PII may be stored in a room/area that has access control measures that prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock or card reader.
- B. Physically secure sensitive PII when in transit. For example, do not pack laptops or electronic storage devices in checked baggage. Do not leave them in a car overnight or in plain sight in a parking lot. Do not mail or courier sensitive PII on CDs unless the CD is encrypted.
- C. Store sensitive PII in shared access computer drives only if access is restricted to those with a need to know by permissions settings or passwords.
- D. Log off, turn off, or lock your computer whenever leaving a desk to ensure that no sensitive PII is compromised.
- E. Do not include sensitive PII in the body of an email. Encrypt all documents containing sensitive PII sent via email. Two software programs on TSA systems that support this are Microsoft Office and WinZip.
- F. Do not discuss or entrust sensitive PII to individuals who do not have a need to know. Be conscious of the environment and surroundings when discussing sensitive PII. Do not discuss sensitive PII on wireless or cordless phones unless absolutely necessary.
- G. Do not leave sensitive PII unattended on a network printer, facsimile, or copier. Do not send sensitive PII to a facsimile without contacting the recipient to arrange for its receipt.
- H. Only desktop or laptop computers, removable hard drives, thumb drives, or other storage devices issued or approved for use by the Chief Information Officer (CIO) may be used for storage of sensitive PII. These devices must be secured with authorization and encryption mechanisms or equivalent protection approved by the CIO.
- I. Do not take sensitive PII home or to any non-DHS worksite, in either paper or electronic format unless appropriately secured. Electronic formats must be encrypted. Paper formats must be under the control of the employee or locked in a container. Personal computers may not be used to access, process or store sensitive PII.
- J. Destroy all sensitive PII when it is no longer needed and continued retention is not required. Destruction may be accomplished by shredding, burning, placing in Sensitive Security Information (SSI) disposal bins, or through such other means as will make the sensitive PII in the record irretrievable. Electronic media must be destroyed using methods identified in [TSA MD 1400.3, TSA Information Security Policy](#). Diskettes or other magnetic media must be cleared (i.e. overwritten or zeroed) before re-use. Records that are stored pending a scheduled

destruction must be safeguarded to prevent unauthorized access during the interval before destruction.

- K. Report any suspected or confirmed loss, theft, or unauthorized disclosures of sensitive PII within one hour of discovery to your supervisor or Program Manager, the Office of Privacy Policy & Compliance (TSAprivacy@dhs.gov), and the TSA Computer Security Incident Response Team (TSA-CSIRT@tsa.dhs.gov). Report the date/time the data compromise was discovered, how it occurred, what data was involved, the number of individuals whose data was compromised, and any information regarding mitigation of the risk of loss (e.g., encryption).
- L. Certain PII, while not sensitive PII, may nevertheless constitute Sensitive Security Information (SSI) under 49 C.F.R. Part 1520 and should be marked and handled in accordance with SSI requirements. PII also constituting SSI is specified as:
 - (1) Lists of the names or other identifying information that identify persons as:
 - (a) having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel;
 - (b) holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport; or
 - (c) holding a position as a Federal Air Marshal.
 - (2) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.