

## **Confidentiality Obligations Acknowledgement and BTS Training Certificate for Access To Bureau of Transportation Statistics & Other Confidential Data**

The success of BTS' information collection operations depends upon the voluntary cooperation of individuals, establishments, and state and local governments to provide the information. BTS' stewardship and protection of confidential information depends on the efficacy of how well the agency implements confidentiality and information system security procedures and the care and vigilance of its employees and contractors.

### **I. Protection of Confidential Information**

BTS collects much of its information under a pledge of confidentiality. Thus, the information must be kept confidential and only used for statistical purposes. The BTS confidentiality statute (49 U.S.C. § 6307(b)) provides that no information may be used for a non-statistical purpose and the information cannot be released in any manner that would disclose a respondent's identity.

BTS employees and contractors must protect confidential information from unauthorized disclosures. Willful, unauthorized disclosure of confidential information is punishable under the following laws:

- **Confidential Information Protection and Statistical Efficiency Act - CIPSEA (44 U.S.C. §§ 3561--3583):** Any employee or contractor who willfully discloses confidential information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and imprisoned for not more than 5 years, or fined not more than \$250,000, or both.
- **Disclosure of Confidential Information (18 U.S.C. § 1905):** Any officer or employee who publishes, divulges, discloses, or makes known in any manner confidential information shall be fined under this law or imprisoned not more than one year, or both; and shall be removed from office or employment.
- **Privacy Act of 1974 (5 U.S.C. § 552a):** Any officer or employee who has access to agency records which contain individually identifiable information and willfully discloses the information in any manner shall be guilty of a misdemeanor and fined not more than \$5,000.

### **II. Security of Information Systems**

Much of BTS' information is designated as "highly sensitive" and confidential. This information must have adequate security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information.

All BTS employees and contractors who administer, control, process, or use confidential information on BTS information systems are responsible for the security and integrity of the information under the following laws:

- **Physical Safeguard of Records (5 U.S.C. § 552a(e)(10)):** Administrative, technical, and physical safeguards must be in place and carried out by staff to insure the security and protection of confidential records against any anticipated threats or hazards to their security or integrity.
- **Federal Records Management (44 U.S.C. 3106):** The unlawful removal or destruction of Federal records is prohibited and is punishable by a fine or imprisonment (18 U.S.C. 2071 and 18 U.S.C. 641). Removal of such records will be reported to the Director of BTS or the BTS

Attorney Advisor. If records are removed from BTS or a contractor site improperly, steps will be taken to have the records recovered.

**III. Whistleblower Protections (5 U.S.C. § 2302(b)(13))**

The provisions of this Confidentiality Obligations Acknowledgement form are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

**IV. Acknowledgement of Responsibilities**

Your signature below indicates that you have received confidentiality training and that you have carefully read and understood your obligations and responsibilities as a BTS employee under the above statutes regarding your access to BTS confidential data. You further acknowledge that if you violate the confidentiality provisions of CIPSEA Sections 513 or make an unauthorized disclosure, you may be found guilty of a class E felony and can be imprisoned up to five years, and/or fined up to \$250,000, or both. You also understand that violations of information system security and practices may lead to reprimand, dismissal, and civil or criminal prosecution. If you have any questions concerning this form or your responsibilities under the various Federal statutes, please contact the BTS Attorney Advisor or BTS Confidentiality Officer. **This form must be signed and returned to BTS.**

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date of Confidentiality Training

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Organization / Phone Number

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
E-mail

Confidentiality Training Provided by: Clara Reschovsky, BTS Confidentiality Officer