U.S. Department of Transportation
Office of the Secretary of Transportation

Bureau of Transportation Statistics

FLOW

Freight Logistics Optimization Works

Confidentiality Manual

Version 2, June 2023

Revision History

Date	Description of Revisions
June 2023	Added section on Entry/Exit procedures

Table of Contents

1. Introduction

The Freight Logistics and Optimization Works (FLOW) program is a joint government and industry initiative aimed at enhancing information-sharing within the freight community. In the FLOW program, individual industry participants provide specific data elements to the Bureau of Transportation Statistics (BTS). As a federal statistical agency, BTS must meet both its mission requirements to collect and disseminate high quality transportation information and its legal and ethical obligations to respect the privacy of those who have provided the information. When BTS collects information for a statistical purpose under a pledge of confidentiality, as it does for the FLOW program, BTS is required by law to protect the information. FLOW participants must be able to trust that the information they provide to BTS will be protected and not be subject to unauthorized disclosure. For that reason, BTS implements confidentiality procedures to prevent the unauthorized disclosure of identifiable information.

BTS protects the confidentiality of FLOW data under various laws described in Appendix A, including the BTS confidentiality statute and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).

This manual contains data confidentiality policies and procedures for the operation of the FLOW program. These apply to:

- All BTS information collected under a confidentiality pledge, as required by law, or through proprietary agreements, and
- All BTS employees, contractors, and agents

2. Scope of Confidential Information

BTS collects, stores, and protects from unauthorized disclosure the following information for the FLOW program:

- FLOW data files submitted by companies
- Information collected by BTS analysts during data-related meetings with companies
- BTS-generated reports for data analysis team review

In addition to the data submitted by FLOW participants, BTS protects the following information from unauthorized disclosure:

- The name of the submitting company
- Any other detail that that would facilitate identification of the submitting company
- Information submitted by each company

In certain circumstances BTS will work with the company to allow for release of their

submitted information to the other FLOW participants as part of an aggregated calculation. The determination will be made in consideration of the usefulness of the data to all participants and concerns of protecting the data submitted by an individual participant. Because FLOW data is collected under BTS's confidentiality statute, BTS has the authority to make final decisions on what information can be released. BTS may take input from affected stakeholders to help determine the sensitivity of any information.

3. Notice of Approval for the Information Collection Request (ICR)

When collecting information, all reporters must be notified that BTS has approval from the Office of Management and Budget (OMB) for the Information Collection Request (ICR). The ICR includes a description of the collection and its planned use as well as other information that demonstrates that BTS has met the requirements of the Paperwork Reduction Act (PRA). Information about the collection must be published in the Federal Register and described in the ICR.

Any notice of approval for the Information Collection Request (ICR) must include the following information:

- The authority (statute or Executive Order of the President) that permits the information collection
- The OMB number that authorizes BTS to collect the information
- The expiration date of BTS's authority to collect the information
- Whether the information collection is mandatory or voluntary
- The principal purpose for the use of the information
- The effects, if any, of not providing the requested information
- Any plans to release identifiable information and the need for reporter consent to release that information

BTS can only use the collected information as described to the reporter in the ICR notice. Approved information collections for the FLOW program include:
OMB Control Number 2138-0049

4. Security Procedures

4.1 Keeping Information Systems Secure

BTS protects its information systems, including server-based, desktop, and laptop computers, from unauthorized access and theft. The security and protection of information systems is standard operating procedure as established by Department guidelines and BTS. The BTS private network, ADBTS, can only be accessed from inside BTS secure rooms.

The BTS Facilities Manager, Confidentiality Officer, and Privacy Act Officer coordinate physical

safeguards of information systems to prevent unauthorized access. BTS staff, contractors, and agents must take all reasonable precautions to protect BTS information systems by:

1. Maintaining all confidential microdata and work products within the BTS private network.
2. Keeping server-based workstations in the BTS secure rooms.
3. Restricting physical access to the BTS secure rooms to authorized staff working directly with FLOW data.
4. Limiting the number of staff with server password access.
5. Not sharing passwords for ADBTS*.
6. Keeping backup tapes or disks under lock and key.
7. Locking office doors during non-work hours or whenever the office is unoccupied, as well as locking laptop computers to a desk.

*ADBTS is an independent network hosted in the DOT HQ Data Center while being completely separate from the DOT HQ network. The application and database servers and the network devices are held in a dedicated, locked cabinet. From within the DOT network, only the web applications hosted on ADBTS can be accessed through standard HTTPS secured connections with the same restrictions over internet connections. However, from the BTS secure rooms, the workstations connect directly to servers in the SFC Data Center. This way, BTS team members can manage the applications, databases, and web servers for the FLOW program.

By remaining a distinct entity from the DOT HQ network, ADBTS maximizes data security and reporter confidentiality. Keeping web applications, databases, files, and other resources within a separate network reduces the risk of human mistakes that can expose sensitive data via the DOT HQ network.

4.2 Keeping Confidential Information Physically Secure

Federal law requires BTS employees, contractors, and agents to protect all confidential information from unauthorized disclosure, theft, and/or accidental loss or misplacement. BTS must take all reasonable precautions to protect the information from unauthorized disclosure. The FLOW program depends on the trust of data providers, and that trust must be maintained.

BTS uses the following procedures when handling FLOW data files:

- All FLOW data files with identifying information must reside within the BTS private network.
- If any physical copies of records are collected, keep any such records with direct identifiers (names, addresses, or other unique identifiers) in the BTS secure rooms'

locked fireproof cabinets.

- Do not store electronic copies of records with direct identifiers on personal computers, servers, or mainframes.
- Do not release confidential records with direct identifiers to anyone outside BTS.
- Do not release records stripped of direct identifiers but not approved for public use to anyone other than FLOW participants or BTS employees, contractors, or agents authorized to access such records.
- Keep records and their copies with direct identifiers only as long as they are needed to carry out the project requirements. Access to them should be restricted to the smallest number of staff consistent with operational functions. A written justification for keeping files with direct identifiers must be given to the BTS Confidentiality Officer, and the justification must include a statement specifying the time period for continued access.
- Transfer internal information (records stripped of direct identifiers but not approved for public use) to the National Archives in sealed containers. The storage center must be advised that no one may access these records except as authorized by the signature of the BTS Director.
- In contracts, specify that BTS contractors must protect confidential information from unauthorized disclosure. Contracts for information collections or processing must contain language that details the procedures and safeguards that BTS uses to protect confidential information.
- Printing, if any, of confidential information will be done only on a printer in a BTS secure room. Any printed information will not be removed from the secure room.
- Do not send or receive confidential information in e-mails or as attachments to e-mails unless the attachments are encrypted.
- Do not place confidential information on public web-based sites.

5. Authorized Access

5.1 BTS Access

Access to original FLOW data files is granted only to BTS employees and contractors who process the reports as part of their assigned duties. Not all BTS staff have access; only those with a need to know because they are assigned to work on the FLOW program may access the FLOW data files. All BTS staff and contractors working on the FLOW program must receive confidentiality training and sign a non-disclosure agreement.

Designated BTS agents may be granted access to confidential information for a limited time under the following conditions:

- A written request for access has been presented to the FLOW Project Officer.
- The extent of data requested has been clearly specified.
- The BTS agent has completed confidentiality training and signed a non-disclosure

agreement.
- The Confidentiality Officer has determined that the BTS agent has a justifiable need to access the confidential information.

5.2 FLOW Participant Access

FLOW participants may not access original FLOW data files other than their own. FLOW participants will access aggregated, de-identified data files and data products via the secure FLOW Data Portal, discussed further in section 6.1. FLOW participants must have an authorized user account to access the portal.

FLOW participants must maintain the confidentiality of all FLOW data files and data products released to participants. Further, FLOW participants must ensure that any third-party accessing FLOW data or products also keeps FLOW data files and products confidential, consistent with the below paragraph excerpted from the FLOW memorandum of agreement between BTS and each participant:

> "Each Participant shall… Ensure any third-party accessing FLOW Data or Products for research, development, analyses, conclusions, or other capabilities commissioned by the Participant abides by the terms of this Agreement. Third party access must be limited to a specific period of performance and is not allow for a long-term pass-through of FLOW Data that circumvents this Agreement or BTS data release processes. **BTS MUST APPROVE ALL THIRD-PARTY ACCESS TO FLOW DATA PER CIPSEA PRIOR TO SUCH ACCESS.** The contracting Participant and/or third party must clearly indicate on all outcomes based on FLOW Data that these Products and results are not guaranteed, sponsored, warranted, or endorsed by the USDOT."

5.3 Interagency Use

BTS may allow another agency access to confidential information only with the consent of the respondent and under written agreement with the institution receiving the information. The interagency transfer of confidential information may occur within the scope of law, only with the express approval of the BTS Director. Before the interagency transfer of confidential information, BTS must inform FLOW participants regarding:

- BTS's intent to share information to an outside agency
- The expected extent of the information shared
- The purpose for sharing the information
- The right to decline or consent to the release of information

Three principles govern BTS action after the initiation of an authorized agreement that allows access to confidential information:

1. The action leading to access must be clearly within the scope of relevant laws and regulations. If there is any doubt, DOT's Office of General Counsel resolves any questions.
2. BTS must inform FLOW participants as to who has access to individual responses and for what purposes the information is collected.
3. BTS must acquire the consent of FLOW participants before giving access to confidential information.

5.4 Potential Public Use

Any public use files that may be developed in the future would contain only aggregated or derived, de-identified data and measures. Prior to release, any public use files must undergo the Disclosure Review Board process, described in section 6.2.

5.5 FLOW Entry and Exit Procedures

Entry into FLOW program
FLOW participation is voluntary. To be included in FLOW and have access to aggregated data, a participant must contribute data to the program. As part of the initial onboarding process, a participant and BTS will agree on a Memorandum of Agreement spelling out the responsibilities of both parties. Once included in the program and contributing data, participants will have access to aggregated FLOW data. This data will not reveal any one participant's data; rather, it will provide aggregated information related to the movement of containers and available supply chain assets at major trade hubs and other locations.

For more information on joining FLOW, please visit www.bts.gov/FLOW.

Departure from FLOW program
A participant may choose to leave the FLOW program or circumstances may arise that require the participant to leave the program for a specified period of time. The conditions and circumstances for conditions of departure are detailed below.

Planned Exits: A participant may formally leave FLOW by communicating with the BTS FLOW Program Manager. The Program Manager will guide the participant through the process of exiting the FLOW program. Data submitted by the participant will continue to be a part of the aggregated FLOW dataset; this is necessary due to the confidential nature of the data submitted into FLOW by all participants. Participants who choose to leave the program will also lose access to the aggregated data in the FLOW dashboard. This does not change the commitment of the exiting participant to keep any aggregated FLOW data confidential. FLOW participants may also be required to sign a departure certificate of non-disclosure.

Data Gaps: There may be situations where participants do not submit data as expected. BTS wishes to avoid these situations whenever possible, particularly to maintain the robustness of the data to allow for aggregated reporting in the FLOW dashboard. There may be instances where a

missing submission could impact the timeliness of data releases.
In these cases, BTS will communicate directly with the participant to explore options for resuming expected data submissions. Reasons contributing to missed submissions could include SFTP transmission errors or staff unavailability. BTS FLOW staff will work with participants to avoid submission gaps and to rectify any missing submissions quickly and to the extent possible by the next regularly scheduled submission date. For situations where past data cannot be submitted due to the nature of how the participant's data is maintained, then their submissions must be brought up to date. As necessary, BTS FLOW staff will try to provide technical solutions to facilitate regular data submissions. If negotiated deadlines are missed and the situation cannot be rectified, then the BTS FLOW Program Manager, in consultation with the BTS Confidentiality Officer, will notify the participant of the unplanned exit procedures (below).

Unplanned Exits: Instances where a participant stops regularly submitting data and a resolution cannot be reached will result in removal of the participant from the program. If this situation arises, BTS will retain the previously submitted data in the FLOW aggregated dataset and the participant will no longer have access to the dashboard with the aggregated data. As with planned exits, an unplanned exit does not change the commitment of the exiting participant to keep any aggregated FLOW data confidential. The exiting participant may also be required to sign a departure certificate of non-disclosure.

Other circumstances that may lead to an unplanned exit involve repeated late data submissions. How "late" is defined will vary based on the cadence of expected submissions; typically, submissions are provided on a weekly basis via portal or daily via SFTP. BTS may agree to an alternate submission cadence on a case-by-case basis. Instances of repeated late submissions in which a resolution cannot be reached will be treated as an unplanned exit from the program.

Reentry into FLOW: Any participant who leaves the program in a planned exit may rejoin at any time if they provide data for the missing period or an agreed upon time-period with BTS FLOW staff. Once they rejoin and submit data, the participant will regain access to the FLOW dashboard and aggregated data.

If a participant left FLOW as part of an unplanned exit, that participant may rejoin by entering into a new MOA with BTS. This agreement will include safeguards to protect against the circumstances that led to their removal from FLOW. Otherwise, the participant will need to meet the same requirements as a participant who rejoins FLOW after a planned exit.

It is expected that these procedures will be further refined through the life of the FLOW program.

6. Disclosure Review Process

6.1 Release of Data to Participants

BTS will utilize a systematic protocol for the release of data and information to participants. All data will be aggregated and de-identified prior to release. Data and information to be released

must meet established criteria. These criteria will be evaluated at both the measure level and the node level.

- Measure refers to the FLOW ratio relevant to the data, including the ratio itself, its numerator, and its denominator.
- Node refers to the geographic location of the data, such as the port or region.

For each measure and node, BTS will evaluate the data to be released and determine whether it is in identifiable form. Under CIPSEA, the term "identifiable form" means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means. Each component of the measure (i.e., ratio, numerator, and denominator) will be evaluated separately. Those components that meet the criteria for disclosure will be released.

- The ratio alone is an aggregated statistic. In general, the ratio can be released to FLOW participants without risk of identification if the numerator and denominator are not readily available elsewhere.
- The numerator and denominator represent counts of supply and demand with potential for attribution if disclosure criteria are not met.

In general, for each measure and node, BTS requires at least three contributors with balanced representation, otherwise all impacted participants must provide their informed consent to release any data that could be identifiable. The thresholds for balanced representation may require input from participants on acceptable levels of representation at each node. Additional release criteria may be established for each measure to ensure confidentiality and data quality. BTS may also apply disclosure limitation methods, described in section 6.3.

Following the determination that a measure has met the criteria for release to FLOW participants, BTS will continue to monitor the measure to ensure it meets disclosure criteria. Gaps in data submissions may prevent the timely release of the FLOW aggregated data, which is part of the reason why regular data submissions are important to the success of FLOW for all participants. Changes that could trigger further disclosure review include changes to FLOW participants (e.g., new participating companies), or changes to distribution ofFLOW data among participants.

In addition to monitoring, BTS will periodically review release criteria to verify it is acceptable and sufficient to protect confidentiality and ensure data quality.

6.2 The Disclosure Review Board (DRB)

In general, for data collected under a pledge of confidentiality, BTS puts in place additional procedures that the agency must follow prior to releasing any public use data files. As the FLOW program matures, if any FLOW public use data files are developed, BTS will convene a Disclosure Review Board (DRB) to review the files prior to their publication. The FLOW Project Officer must implement any disclosure limitation methods required by the DRB or the BTS Confidentiality Officer.

DRB membership is limited to federal employees. The BTS Confidentiality Officer, a senior statistician with experience and knowledge on confidentiality and disclosure limitation methods, heads the DRB. In addition to the BTS Confidentiality Officer, members of the DRB include: BTS staff members, and an external member from another federal statistical agency (such as the U.S. Census Bureau), if available. FLOW Project Officer in coordination with the BTS Confidentiality Officer can seek others with relevant expertise to assist DRB in its evaluation.

6.3 Disclosure Limitation Methods

If BTS collects information under confidentiality laws or a pledge of confidentiality, as it does for the FLOW program, BTS must review any information to be disclosed for potential disclosures of confidential information. If potential disclosures are identified, BTS staff apply disclosure limitation methods to the information to mitigate disclosure risk before any release.

Disclosure limitation methods can be global or unique. Global methods include deletion, in which direct identifiers are removed, and fixed transformation, in which possible indirect identifiers are replaced by a fixed generic term or higher levels of aggregation. An example of a unique method is variable transformation, in which occurrences of possible indirect identifiers are transformed in different ways depending on the context and structure of the data description.

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) requires that a respondent's identity must not be disclosed directly or indirectly. FLOW data must be aggregated and de-identified under CIPSEA.

Aggregated and de-identified data files have the following characteristics:

- They include no direct identifiers, such as company name.
- All included variables have been reviewed for potential indirect identification in accordance with the disclosure review procedures.

7. Confidentiality Training

Confidentiality training focuses on laws, procedures, and security. This training makes sure that BTS employees, contractors, and agents understand their responsibility to protect confidential information. New BTS employees, contractors, and agents participate in confidentiality training as soon as possible after they are employed or start working on BTS projects. At the completion of confidentiality training, BTS employees, contractors, and agents must sign a non-disclosure agreement.

Annual confidentiality training is required for all current BTS employees, contractors, and agents. The BTS Confidentiality Officer develops the content for confidentiality training, conducts the confidentiality training, and keeps all signed non-disclosure agreements. When a BTS employee, contractor, or agent leaves BTS, they must read and sign a Departure Certification for Non-Disclosure of Confidential Information form. These forms are held by the BTS Confidentiality Officer.

8. Penalties for Unauthorized Release of Confidential Information

Willful unauthorized disclosure or use of BTS confidential information violates federal law. Such unauthorized disclosure or use of confidential information by a BTS employee, contractor, or agent may constitute cause for BTS to take disciplinary action against that employee, including reprimand, suspension, demotion, or removal from office. Other possible sanctions could include fines or imprisonment.

BTS's stewardship and protection of confidential information depends on the efficacy of employees, contractors, and agents implementing this manual's procedures with care and vigilance. Each employee, contractor, and agent must protect confidential information and use the information only for the purposes for which it was collected.

The statute which governs BTS confidentiality is the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). This statute prohibits disclosure or release, for non-statistical purposes, of information collected under a pledge of confidentiality. Under CIPSEA, data may not be released to unauthorized persons. Willful and knowing disclosure of protected data to unauthorized persons is a felony punishable by up to five years imprisonment and up to a $250,000 fine.

9. Responding to Requests for Data

If a BTS employee or contractor working with FLOW receives a request for information that cites the Freedom of Information Act (FOIA), they should immediately refer this request to the OST-R FOIA Officer and the BTS Confidentiality Officer.

In general, FOIA requires that federal agencies provide copies of the requested information. However, there are two important exemptions from Section 552(b) of FOIA:

- Subsection (b)(3) excludes matters "specifically exempted from disclosure by statute" from the disclosure requirement.
- Subsection (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

BTS's confidentiality statute (49 U.S.C. 111(i)) and the Confidential Information and Statistical Efficiency Act (CIPSEA, Title III of the Foundations for Evidence-Based Policymaking Act, P.L. 115-435)) are statutory exemptions to FOIA requests. FLOW data are protected from disclosure under FOIA.

10. Glossary

BTS Secure Room: a controlled access space in which only staff members authorized by the

Project Officer may enter

Confidential: a status given to sensitive information that must be protected

Confidential Information Protection and Statistical Efficiency Act (CIPSEA): Enacted in 2002 and reauthorized in the Foundations for Evidence-Based Policymaking Act of 2018 (Pub. L. 115-435); provides strong confidentiality protections to information collected for statistical purposes by Federal Agencies

Confidentiality pledge: a guarantee to the reporter that BTS limits its use of the information to stated purposes and protects the information from unauthorized disclosure; part of the Information Collection Request (ICR)

Disclosure: an occurrence that releases confidential information about a reporter to a third party

Approximate disclosure: when a characteristic that falls in a range (such as being between 45 and 55 years of age) is released

Authorized disclosure: when a respondent has consented to the release of information

Exact disclosure: when a specific characteristic (such as a reporter's race, sex, or age) is released

External disclosure: when outside data is linked or merged into data from another study in a way that releases sensitive information

Inadvertent disclosure: when a tabulation or file available to the public releases or can release information given by a reporter

Internal disclosure: when information is released from only one study

Probability-based disclosure: when data in a table indicates that members of a given population segment has a high probability of having a certain sensitive characteristic

Unauthorized disclosure: when information is intentionally released to a third party without the reporter's consent

Disclosure limitation method: a statistical method applied to an information product to reduce the risk of disclosing confidential information before public release

Disclosure Review Board (DRB): a group of federal staff within BTS and an external federal member who review BTS information products for the disclosure of confidential information

Identifying information: information that directly identifies a respondent (such as a name,

address, or identification number) or that can indirectly identify a reporter when linked to other unique details (such as a combination of gender, race, date of birth, and geographic indicator); also called a direct or indirect identifier

Information Collection Request (ICR): a notification given to reporters before collecting any information

Informed consent: an acknowledgment by a respondent that they agree to the collection, publication, or other use of the information given to BTS

Intruder: any individual or group who attempt to use information products to determine the identity of the reporters who gave the information

Microdata: data gathered on a very small scale (such as for an individual)

Non-statistical purpose: the use of identifying information for any purpose that is not statistical in nature, including but not limited to administrative, regulatory, law enforcement, or adjudicatory purposes that affect the rights, privileges, or benefits of a particular reporter; includes the disclosure of information under the Freedom of Information Act (FOIA)

Privacy: the right of reporters to control the use and disclosure of information about themselves

Reporter: a respondent; an entity that gives information to BTS for FLOW; may be a person, business, or corporation

Security: the administrative and physical safeguards that protect confidential information from unauthorized disclosure and limits access to authorized users only;

Statistical purpose: the use of information to describe, estimate, or analyze the characteristics of groups without identifying individuals

Appendix A. Overview of Confidentiality Laws

BTS Confidentiality Statute, 49 U.S.C. 6307(b)

Title 49 of the United States Code, Section 6307(b) provides the basic legal requirement for protecting a respondent's identity in BTS information collections. It reads:

> (b) Prohibition on Certain Disclosures.—
>
> (1) In general.—An officer, employee, or contractor of the Bureau may not—
>
> (A) make any disclosure in which the data provided by an individual or organization under section 6302(b)(3)(B) or section 6314(b) can be identified;
>
> (B) use the information provided under section 6302(b)(3)(B) or section 6314(b) for a nonstatistical purpose; or
>
> (C) permit anyone other than an individual authorized by the Director to examine any individual report provided under section 6302(b)(3)(B) or section 6314(b).
>
> (2) Copies of reports.—
>
> (A) In general.—
>
> No department, bureau, agency, officer, or employee of the United States (except the Director in carrying out this chapter) may require, for any reason, a copy of any report that has been filed under section 6302(b)(3)(B) or section 6314(b) with the Bureau or retained by an individual respondent.
>
> (B) Limitation on judicial proceedings.—A copy of a report described in subparagraph (A) that has been retained by an individual respondent or filed with the Bureau or any of the employees, contractors, or agents of the Bureau—
>
> (i) shall be immune from legal process; and
>
> (ii) shall not, without the consent of the individual concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings.
>
> (C) Applicability.—
>
> This paragraph shall apply only to reports that permit information concerning an individual or organization to be reasonably determined by direct or indirect means.
>
> (3) Informing respondent of use of data.—
>
> If the Bureau is authorized by statute to collect data or information for a nonstatistical purpose, the Director shall clearly distinguish the collection of the data or information, by rule and on the collection instrument, in a manner that

informs the respondent who is requested or required to supply the data or information of the nonstatistical purpose.

In data collections for statistical purposes, such as FLOW, under the above statute:

- Employees and contractors of BTS may not disclose the identity of any respondent.
- Information collected is limited to statistical research and reporting only.
- No one can have access to any report or record (except authorized BTS employees) unless authorized by the Director.

Disclosure of identifying information of a respondent is understood to be any information which can be used to establish the identity of a respondent directly or indirectly.

The second clause states that no department, bureau, agency, officer, or employee of the United States may require a copy of any report or record. However, the Director of BTS may allow confidential information to be shared under an agreement approved by the Director. Any information (report or record) filed with BTS is also immune from legal processes and cannot be admitted as evidence in any court action, suit or other judicial or administrative proceeding unless such use is approved in advance by the concerned individual.

These restrictions apply to direct and indirect identifying information.

The third clause directs BTS Director to clearly identify information collections, in which the use of the information will be for a non-statistical purpose. This notification should appear in the Federal Register announcement and on the information collection instrument.

Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

CIPSEA is contained in the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Public Law 15-435, Title III. CIPSEA establishes several requirements for Federal agencies when they collect information under a pledge of confidentiality for exclusively statistical purposes from individuals or organizations. An agency must make sure that the information collected:

- Be used only for statistical purposes;
- Is not disclosed in identifiable form to anyone not authorized by Title III; and
- Is safeguarded by controlling access to, and uses of such information.

The Act states that data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form and can only be used for statistical purposes (e.g., not regulatory or enforcement actions), except in cases where the agency has received the informed consent of the respondent.

When a statistical agency or unit collects information for a non-statistical purpose (e.g., BTS's

Office of Airline Information (OAI) data collection program), it must give notice to the public and clearly distinguish information collected for a non-statistical purpose from information collected for a statistical purpose.

CIPSEA contains fines and penalties for unauthorized disclosures of information collected under a pledge of confidentiality where the information is designated exclusively for statistical purposes. If an officer, employee, or agent of the agency (e.g., a contractor or a contractor's employee) knowingly and willfully discloses the information in any manner to a person or agency not entitled to receive it, they are guilty of a class E felony and imprisoned for not more than 5 years, fined not more than $250,000, or both imprisoned and fined.

CIPSEA does not restrict or diminish any confidentiality protections or penalties for the unauthorized disclosure of information that are contained in other statutes. Therefore, CIPSEA does not diminish or override the current prohibitions against disclosing confidential information found in BTS's confidentiality statute.

Privacy Act of 1974, 44 U.S.C. 3106 Section 552a

The Privacy Act provides for the confidential treatment of records of individuals that are maintained by a Federal agency according to either the individual's name or some other identifier. This law also requires that BTS protect these records from uses other than those purposes for which they were collected. It further requires agencies to:

- Collect only that information necessary to perform agency functions,
- Publish descriptions of existing data systems (called "systems of records") so that the public can learn what records are maintained by the agency,
- Inform individuals at the time of information collection as to the legislative authority under which it is requested, whether the request is mandatory or voluntary, the consequences, if any, of non-response, and the purposes and uses to be made of the information,
- Maintain no records on how an individual exercises his rights under the first amendment except with special legal authorization,
- With certain exceptions, permit individuals to examine records maintained about themselves and to challenge the accuracy of those records,
- Establish rules of conduct governing persons involved in collecting and maintaining records, and
- Establish appropriate administrative, technical, and physical safeguards to protect records.

Employees and contractors of Federal agencies are subject to this Act, and anyone who willfully discloses personal information contrary to this law or who fails to give notice of a system of records may be fined and the agency may be sued for damages.

The Act also places severe restrictions on the use of an individual's social security number, such

that BTS is precluded from using social security numbers for anything but statistical activities that are clearly explained to respondents.

Federal Law Governing Federal Employees' Behavior, 18 U.S.C. 1905

This law includes the following provision, which is relevant to protecting BTS confidential information:

> Disclosure of confidential information…Whoever, being an officer or employee of the United States or of any department or agency thereof…publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.
>
> Employees and contractors of federal agencies are subject to this Act, and anyone who willfully discloses any confidential information, which is contrary to this law, could be fined, imprisoned, or both fined and imprisoned.

Freedom of Information Act (FOIA), 5 U.S.C. 552

This Act was first passed in 1967 and amended in 1974 and 1996. FOIA requires federal agencies to make their records available to persons who request them. Some have speculated that this law undoes the privacy protection required under the laws cited above. However, several kinds of information are specifically exempted from the disclosure requirements of the FOIA. Two exclusions provided in Section 552(b) of the Act are relevant to CCDP:

- Subsection (b)(3) provides that matters "specifically exempted from disclosure by statute" are also excluded from the disclosure requirement, and
- Subsection (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

BTS' confidentiality statute (49 U.S.C. 111(i)) represents a statutory exemption to FOIA requests. Therefore, BTS confidential records and information are protected from disclosure under FOIA. Additionally, information collected under the provisions of CIPSEA are expressly limited to use for a statistical purpose and may not be disclosed for another purpose without prior consent of the responder.

Appendix B. Respondent Notification Statements

Burden Statement

A federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a current valid OMB Control Number. The OMB Control Number for this information collection is 2138-0049. It is anticipated that companies will submit present-time data periodically, as frequently as daily, with each submission requiring approximately 15 minutes for data gathering and submission. Reporting any information to the FLOW program is voluntary. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: Demetra Collia, US DOT/ BTS, 1200 New Jersey Avenue SE, Room E36-302, Washington, D.C. 20590 or e-mail: Demetra.Collia@dot.gov or btsdataportal@dot.gov.

Confidentiality Pledge

The information you provide will be used for statistical purposes only. In accordance with the BTS confidentiality statute (49 U.S.C. 6307) and the provisions of the Confidential Information Protection and Statistical Efficiency Act (Title III of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435), your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than BTS employees or BTS agents. In accordance with these confidentiality statutes, data you submit will be used exclusively for statistical purposes and will not be disclosed in identifiable form except with the informed consent of the respondent. By law, every BTS employee and BTS agent has taken an oath of confidentiality and is subject to a jail term of up to 5 years, a fine of up to $250,000, or both if he or she discloses any identifiable information about the respondent or reporting company or operator.