

Data Protection in the Confidential Close Call Reporting System

J. Neil Russell, Ph.D.
Confidentiality Officer



U.S. Department of Transportation
Bureau of Transportation Statistics



Overview

- FRA's Confidential Close Call Reporting System (C³RS) features.
- Why use a 3rd party data collector?
- Which laws protect the data?
- How do the laws protect the data?
- What are the internal procedures for protecting the data?

C³RS Features

- **Legal constraints are in place to ensure the confidentiality of the data provider and their employer.**
- **Confidentiality of data provider encourages reporting of close calls.**

3

C³RS Features

- **A neutral third party will collect, maintain, and protect the data to ensure confidentiality.**
- **Close call data are not collected by the regulatory agency (FRA) and this should encourage reporting.**

4

Bureau of Transportation Statistics (BTS)

- **BTS is as a Federal statistical agency.**
- **Hence, BTS has an unique law which protect the data it collects.**
- **BTS will serve as the third party data collector for the C³RS.**

5

BTS Data Collection Authority

- **By law^{*}, when BTS collects data, BTS must:**
 - **Pledge confidentiality to data provider,**
 - **Use the data for statistical purposes only,**
and
 - **Protect the data from unauthorized use and release.**

*** 49 U.S.C. 111(i) and Public Law 107-347, Title V.**

6

Confidentiality Pledge

- **A confidentiality pledge is a guarantee to the data provider that BTS will only use the information for statistical purposes and will protect the information from unauthorized release and use.**

7

Data Use

- **Statistical purpose - the description or analysis of information about groups or subgroups of the economy, society, or environment.**
- **Non-statistical purpose - the administrative, regulatory, or law enforcement use of information affecting the rights, privileges, or benefits of a data provider.**

8

Data Protection

- By law, BTS employees and contractors shall not:
 - disclose any data that could identify a data provider;
 - use the information for a non-statistical purpose;
 - permit unauthorized persons to examine individual reports.

9

Data Protection

- By law, BTS is prohibited from releasing data to:
 - Other government agencies,
 - The courts (data immune from the legal process and cannot be admitted as evidence), and
 - Under Freedom of Information Act (FOIA) requests.

10

Data Protection

- **BTS data collections are also covered under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002.***
- **Under CIPSEA, data cannot be:**
 - Disclosed if it could identify a data provider.
 - Used for any non-statistical purpose.
 - Released under a FOIA request.

* Public Law 107-347, Title V (E-Gov't Act of 2002)

11

Data Protection

- **Penalties for BTS employees and contractors for an unauthorized release or use of confidential data:**
 - Reprimand, suspension, demotion, or removal from office, and
 - Class E felony with up to 5 years in prison and/or \$250,000 fine.

12

Data Protection Procedures

- All BTS employees and contractors must:
 - Participate in annual confidentiality training.
 - Sign a non-disclosure affidavit.
 - Have all project related documents reviewed to ensure confidential data protection.
- BTS implements security procedures to secure its:
 - Information systems and
 - Physical space.

13

Questions ?

Neil Russell

Confidentiality Officer

Bureau of Transportation Statistics

202-493-2147

neil.russell@dot.gov

14