U.S. Department of Transportation

Office of the Secretary of Transportation

Privacy Impact Assessment
Close Call Data System (CCDS)

Responsible Official
Allison Fischman
Bureau of Transportation Statistics
allison.fischman@dot.gov

Approving Official
Karyn Gorman
DOT Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Bureau of Transportation Statistics (BTS) operates and maintains the Close Call Data System (CCDS) to store, process, and access various confidential data collection programs. These data are collected and protected under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title III of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, codified as amended at 44 USC 3561-3583), which requires BTS to protect the trust of providers of information by ensuring the confidentiality and exclusive statistical use of their responses. BTS data collections conducted under CIPSEA include near-miss and safety data collection programs, supply chain and freight-related data collection programs, and certain transportation surveys.

This Privacy Impact Assessment (PIA) is an update to the previously published PIA. It is being updated in accordance with the E-Government Act of 2002 to assess the potential privacy risks associated with the system's operations and ensure compliance with applicable data protection regulations and safeguarding of individuals' personal information. The assessment aims to identify and mitigate privacy risks, ensuring that data handling practices align with legal and organizational standards.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1] Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The CCDS is a system owned and operated by the BTS. It comprises a collection of database, internal-facing applications, and external-facing applications to store, process, and access various confidential data collection programs. Information within the CCDS is provided to BTS by individuals and companies participating in BTS confidential data collection programs, which include transportation safety data collection programs, supply chain and freight-related data collection programs, and certain transportation survey programs. These data are protected under BTS's confidentiality statute (49 U.S.C. 6307(b)) and the Confidential Information Protection and Statistical Efficiency Act of 2018 (44 U.S.C. 3561–3583), also known as Title III of the Foundations for Evidence-Based Policymaking Act of 2018. CIPSEA requires BTS to protect the trust of information providers by ensuring the confidentiality and exclusive statistical use of their responses. BTS must protect the identity of the respondent and treat reports confidentially. Information submitted under CIPSEA is also protected from release to other government agencies, exempt from Freedom of Information Act (FOIA) requests, and immune from legal process. BTS employees, contractors, and agents are subject to strict criminal and civil penalties for noncompliance (up to 5 years imprisonment and $250,000 fine).

The primary purpose of the CCDS is to facilitate the full cycle of BTS confidential data collection program operations, from data collection to data processing and analysis, to production, publication, and dissemination of analytical reports, dashboards, special topic reports, and other informational materials. A typical transaction within the system involves a user completing a survey or a program participant submitting a data report or a batch data transfer via CCDS data collection applications, such as online survey forms, online report submission portal, or secure file transfer protocol (SFTP). BTS analysts or subject matter experts

(SME) review, perform quality control of the reports and data collected and produce datasets that are suitable for statistical analysis, and BTS performs statistical analyses and generate statistical reports and products to provide information on topics for which the data are collected to support decision making. Information within the system can be accessed only by BTS-authorized personnel.

The CCDS contains Personally Identifiable Information (PII) and non-PII received from individuals and companies participating in BTS confidential data collection programs in accordance with the specific data collection requirements of the program. For company-level data collection programs, PII collected is limited to name and contact details of the respondent or representative designated to submit data on behalf of their organization. For individual reporting programs such as the confidential close call reporting program, in which transit agency employees report close calls or near miss events to BTS, PII information includes name, employee identification number, and contact details. For this program and other programs involving confidential interviews, BTS uses this information to contact the individual for interviews as needed. No social security numbers are collected through CCDS. PII stored in CCDS is not used as part of BTS statistical analyses.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Most information stored within CCDS is not retrieved or accessed by a unique identifier associated with or assigned to an individual; rather, records are associated with safety events or operational information pertinent to the subject of the data collection. However, some records in the system pertaining to the confidential close calls reporting program are maintained in accordance with the Department's published System of Records Notice (SORN), DOT/ALL 21 - Close Call Confidentiality Reporting System (C3RS) -75 FR 20420 - April 19, 2010. There are no exemptions claimed for the system. The CCDS SORN is made publicly available at http://www.transportation.gov/privacy, and individuals and program participants are encouraged to review it before providing any personal information or data to the system.

As required by the Privacy Act, BTS provides direct notice to individuals participating in confidential data collections via Privacy Act statements on CCDS reporting forms, secure data collection applications, and web portals. Individuals who provide information to the CCDS system are required to acknowledge their understanding of the program's pledge of confidentiality and burden statement at the data collection portal. This acknowledgment is an essential part of the data submission process, ensuring that individuals are fully informed about how their data will be used and the privacy protections in place.

The publication of this PIA demonstrates BTS's commitment to provide the appropriate transparency into the CCDS. This PIA is available to the public at: https://www.transportation.gov/individuals/privacy/privacy-impact-assessments.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Under the provision of DOT Privacy Act/ Freedom of Information Act (FOIA) procedures, individuals may request searches of the CCDS to determine any records that may have been added or pertain to them. The FOIA is a federal law that give you the right to access any U.S. Department of Transportation (DOT) records unless DOT reasonably foresees that the release of the information to those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. DOT reviews all Privacy Act Requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Note that CIPSEA generally prohibits the release of CCDS records under Freedom of Information Act (FOIA) requests. The above paragraph pertains narrowly to an individual's request for information pertinent to themself.

Notification procedure: Requests should be submitted to the attention of the official responsible for the record at the address below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Individuals should include in their requests the following information:

- Name and title of the system of records from which you are requesting the search;
- Name of individual;
- Mailing address;
- Phone number or email address; and
- Description of the records sought.

Contesting record procedure: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for and why the records should be corrected. Requests should be submitted to the attention of the OST Official responsible for the record at the address below:

DOT Chief Privacy Officer
Department of Transportation
1200 New Jersey Ave, SE
E31-312
Washington DC, 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Privacy Act request for records covered by system of records notices not published by the Department will be coordinated with the appropriate customer privacy official and acted upon accordingly.

Additional information about the Department's privacy program may be found at: https://www.transportation.gov/privacy-program/about-us. Individuals may also contact the

DOT Chief Privacy Officer at: privacy@dot.gov. For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

BTS is authorized under 49 USC chapter 63 to collect transportation information for its various program needs. The BTS confidentiality statute (49 U.S.C. 6307(b)) and other laws (18 U.S.C. 1905; The Privacy Act of 1974, and the Confidential Information Protection and Statistical Efficiency Act (44 U.S.C. 3561–3583) protect the information BTS collects. These laws ensure that any identifying, sensitive, or proprietary information that BTS collects is not released to unauthorized persons or organizations.

When BTS collects or acquires information for a statistical purpose under CIPSEA, BTS:

- Must use a pledge of confidentiality,
- Must protect the information and cannot allow unauthorized access to the information,
- May share the information for statistical purposes if the respondent consents, and then only under a written agreement signed by the Director of BTS. The party or agent receiving the confidential information pledges confidentiality and is then subject to the restrictions and penalties provided in CIPSEA,
- Employees, contractors, and agents are subject to felony charges and fines for knowingly disclosing confidential information (5 years prison and/or $250,000 fine), and
- Cannot release the information under a Freedom of Information Act (FOIA) request. The information is also immune from legal process.

The CCDS supports BTS confidential data collection program operations. It is used to collect confidential data; securely store, process, and analyze that data; and provide analyses and learnings that can be used to improve program objectives, such as transportation safety root cause analysis or freight and supply chain system efficiency.

Certain BTS confidential data collection programs conducted under CIPSEA are authorized or required by regulation, e.g., 30 CFR 250.730(c) and 250.803, which require offshore energy operators to submit reports involving critical safety equipment to BTS.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only if necessary to

fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

The CCDS is designed to comply with the principles of data minimization and retention in accordance with the Privacy Act and guidelines from the National Archives and Records Administration (NARA). These principles ensure that the system only collects, uses, and retains PII that is necessary for the specified purpose for which it was originally collected. Additionally, the retention period for PII is strictly limited to what is necessary to fulfill the system's purpose and in alignment with NARA-approved record retention schedules. CCDS manages risk by providing only relevant and necessary PII to conduct, manage, and process confidential data collection programs.

CCDS records are maintained in accordance with NARA records schedule number DAA-0398-2024-0001, Close Call Data System: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0398/daa-0398-2024-0001_sf115.pdf. Under the records schedule, CCDS data files are classified as temporary and are not archived with NARA, with the exception of program outputs such as publications. In accordance with the records schedule, CCDS data files are classified as temporary and are destroyed 15 years after the subject data program is terminated.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

BTS has implemented robust monitoring and auditing mechanisms to ensure that the use of PII remains within the bounds of the specified purposes:

- **Access Restrictions**: Access to CCDS data is restricted based on roles and responsibilities within BTS. Only authorized BTS personnel with need to know are granted access to CCDS data, and access is limited to secure physical or virtual environments.
- **User Authentication**: Multi-factor authentication (MFA) is required for all personnel accessing CCDS data, ensuring that only authorized individuals can interact with sensitive data.
- **Audit Logs**: The CCDS maintains detailed logs of all activities related to the access, modification, or dissemination of data. These logs are regularly reviewed to identify and address any unauthorized access or misuse of data.
- **Data Encryption**: Data encryption is applied to storage and transmittal.

All personnel granted access to CCDS data are required to undergo comprehensive training to ensure they understand the privacy and security responsibilities associated with handling PII and confidential data. These training programs are designed to enhance staff awareness of the importance of PII and confidential data protection, BTS's policies on data use, and the potential privacy risks involved in mishandling confidential data. BTS personnel authorized to access CCDS are also required to sign a nondisclosure agreement. The trainings include:

- BTS Confidentiality and Non-Disclosure Training
- Sensitive but Non-Classified Information Training
- IT Security and Behavior Training

To mitigate privacy risks, BTS strictly limits the sharing of CCDS data. BTS is prohibited from sharing CCDS data, including PII, outside the organization, in accordance with its obligations under the CIPSEA. Further, PII stored in CCDS is not used as part of BTS statistical analyses.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

PII collected from individuals reporting or providing information to CCDS align with the purpose of SORN DOT/ALL 21. Respondents are responsible for ensuring the accuracy and quality of the PII they provide. If BTS learns of PII inaccuracies, the information is updated within the system. BTS reviews CCDS and its confidential data collection programs regulatory to ensure data is accurate, relevant, timely, and complete.

The CCDS has implemented several measures to protect the quality and integrity of data throughout its lifecycle:

- **Access Control**: Strict access control policies are enforced to ensure that only authorized personnel can modify or update sensitive data. Role-based access ensures that individuals can only interact with the data they are permitted to access.
- **Data Versioning**: The CCDS uses version control to track changes to data, preserving historical records of data modifications. This enables the CCDS to maintain the integrity of data and ensure that any updates or changes are documented and traceable.
- **Audit Trails**: Comprehensive audit trails are maintained to log all changes to critical data. These logs capture who made each change, when the change occurred, and the nature of the modification. This provides transparency and ensures that any discrepancies can be traced back to their source.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII collected within CCDS is stored via encrypted means. Access to PII within the CCDS system is restricted to duly authorized personnel based on a strict need-to-know basis. The following conditions must be met for an individual to gain access to the system:

- The individual must have a clearly defined need to access the data based on the mission and operations of BTS.
- The individual must complete the BTS's required confidentiality training and sign the BTS's nondisclosure agreement.
- The individual's access permission must be approved by the BTS Confidentiality Officer and the director of the subject data collection.
- The individual must abide by BTS confidentiality policy and procedures.

PII is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 as revised, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009. The Department has a comprehensive information security program that contains management, operational, and technical safeguards designed to ensure the security, integrity, and confidentiality of PII. This includes annual continuous monitoring assessment that supports reaccreditation and reauthorization of the system, in accordance with OMB Circular A-130's requirement for annual testing.

CCDS is designed, operated, and maintained to meet all current cybersecurity requirements for protecting privacy and confidentiality. Access to data in the CCDS system is monitored to ensure compliance with DOT's security and privacy policies. Authorized users are required to log in using their individual credentials, which are tracked for accountability. Additionally, any changes made to data within the system are logged, capturing details about who performed the change and what modifications were made. This tracking ensures that unauthorized access or alterations are quickly detected and addressed. CCDS is protected from unauthorized access through appropriate administrative, physical, and technical safeguards.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

BTS has established clear organizational structures and policies to oversee the protection of privacy and PII. These governance controls ensure that privacy principles are integrated into all business processes and that privacy compliance is continuously maintained. Key governance measures include:

- **Confidentiality Officer**: BTS has designated a Confidentiality Officer responsible for overseeing the implementation and enforcement of privacy policies, ensuring compliance with OMB guidelines, and serving as the central point of contact for privacy-related matters.
- **Confidentiality Policies and Procedures**: BTS has developed comprehensive confidentiality and privacy policies and procedures to guide the collection, handling, and protection of PII.
- **Regular Training**: To ensure that staff understand their privacy responsibilities, BTS conducts mandatory annual Confidentiality and Non-Disclosure training, which covers concepts of privacy, PII, Privacy Act, what is a privacy disclosure, how individuals can be indirectly identified, and BTS statutory responsibilities for protecting privacy and confidentiality. In addition, BTS employees and contractors are also required to take DOT Privacy Awareness Training annually.

Further, CCDS audit logs are routinely reviewed for anomalies. The CCDS auditing system captures account maintenance and events. The Information System Owner (ISO), Information Systems Security Manager (ISSM), Information System Security Officer (ISSO), and DOT Security Operations Center (SOC) determine any changes required due to the current threat environment.

Responsible Official

Allison Fischman
Information System Owner
Director, Office of Safety Data and Analysis
Bureau of Transportation Statistics

Approving Official

Karyn Gorman
DOT Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2025.10.27 11:45:27 -04'00'