DOT 1351.34A JUNE 23, 2026

Subject: U.S. DEPARTMENT OF TRANSPORTATION DATA MANAGEMENT POLICY

1. PURPOSE.

This Order updates the U.S. Department of Transportation (DOT) policy on data management, which provides high-level directives to which DOT Operating Administrations and Secretarial Offices (collectively, "Components") must adhere throughout the data lifecycle.

2. CANCELLATIONS.

This Order cancels CIO IT Policy (CIOP) Chapter 1351.34, Data Management Policy, dated July 13, 2017. This order also rescinds CIOP Chapter 1370.11 Information Processing Standards Program Policy, dated July 8, 1982.

3. BACKGROUND.

DOT uses data and data assets in support of its work to advance transportation safety and improve operational efficiency. This order enables a structured approach for data governance, and can support robust, evidence-based decision-making and fuel advanced analytics and human-centered artificial intelligence (AI).

DOT has a default posture that ensures data and data assets are designed for maximum long-term value and seamless usability.

This order implements the requirements from legislation, executive branch policies, presidential memoranda, and other leading practices.

4. REFERENCES.

See Appendix A.

5. DEFINITIONS.

See Appendix B.

6. SCOPE.

This order governs the use of data by DOT personnel, including data that DOT collects, stores, acquires, generates under contract, generates using AI, processes, uses, sponsors in research or other financial assistance agreements.[1]

[1] Financial assistance agreements include, but are not limited to grants, loans, cooperative agreements, or other transactions.

This order applies to all DOT Operating Administrations and Secretarial Offices and all DOT personnel.[2]

This order applies to data that DOT gathers from outside parties (*e.g.*, academic and research stakeholders, State, territorial, Tribal governments, non-governmental organizations) if DOT intends to use or disseminate it.

This order applies to statistical agency uses of data collected with a promise of confidentiality under the Confidential Information Protection and Statistical Efficiency Act.[3]

This order does not apply to data that DOT-regulated entities or funding recipients use. In addition to the requirements stated herein, data must adhere to existing Federal laws, DOT policies, and implementation guidance.

7. POLICY.

DOT personnel will a) apply data management lifecycle practices and b) incorporate flexible risk management.

a. Data management lifecycle practices.

Components should apply seven distinct phases (design, collection, storage, processing, dissemination, usage, and disposal of or transfer) during the iterative data management lifecycle. Components may incorporate additional principles, practices, or activities consistent with this order.

1) Collection

a) DOT will ensure data is collected with accessibility, transparency, interoperability, and the end user in mind.
b) DOT will adopt data and metadata standards.[4]
c) DOT will reduce the redundancy of collection efforts and will share data across DOT Components, consistent with applicable laws, regulations, and policies, to the greatest extent practicable through Memorandums of Understanding or Agreement.
d) DOT will seek to satisfy new data needs through interagency, intergovernmental, open sharing, data trusts, open license, or commercial sources before creating or collecting new data, to the greatest extent practicable.
e) DOT will seek the least possible restrictive licensing terms when acquiring data for its own use and will always exercise its data rights to the greatest extent

---

[2] The Office of Inspector General (OIG) is not a Component as defined in this policy but will issue internal policies consistent with this policy. OIG will work with the DOT OCIO when consistent with OIG independence.
[3] The Confidential Information Protection and Statistical Efficiency Act is Title V of the E-Government Act of 2002.
[4] In accordance with OMB Circular A-119, voluntary consensus standards such as ISO19100 for geospatial data and DCAT 3.0 metadata standards in OMB M-25-05.

practicable.

2) Storage

   a) DOT will design, implement, and maintain scalable and resilient data storage architectures that ensure high availability, data integrity, and robust disaster recovery capabilities to support business operations and protect data assets from data loss or corruption.
   b) DOT will implement identity and access management and data encryption standards to ensure data assets are protected against unauthorized access and security vulnerabilities.

3) Processing

   a) DOT will establish and implement processes for pre-dissemination data review and evaluation to continuously improve data quality.
   b) DOT will process data for improved efficiency and effectiveness.

4) Dissemination

   a) DOT will ensure data is open by default, except where prohibited, while following laws, policies, and best practices for privacy, confidentiality, and security.
   b) DOT will apply the least restrictive open license to data and data assets.

5) Usage

   a) DOT will operationalize the FAIR-D (Findable, Accessible, Interoperable, Reusable, and Delightful[5]) framework.
   b) DOT will ensure data is contextually rich with metadata and data dictionaries, to the greatest extent practicable.

6) Disposal of or Transfer

   a) DOT will dispose of or transfer data according to DOT policy and applicable Federal law(s) and retention schedules.

   b) Flexible risk management.

Flexible risk management principles are designed to enable responsible data innovation. The degree of required oversight scales with frequency, persistence, and impact of use.

1) DOT will consider data management risks within the broader context of DOT governance and risk management processes.
2) DOT will foster a safety-first mindset in the design, development, deployment, and use of data to minimize negative impacts.

---

[5] As described in the DOT Open Data Plan.

3) DOT will communicate data activities with an Enterprise Data Inventory.
4) DOT will ensure robust stakeholder engagement processes affecting the public; other Federal agencies; State, territorial, and Tribal governments; and others—are implemented throughout the data management lifecycle, while also maintaining a continuous commitment to improvement.
5) DOT will communicate with stakeholders regarding substantial changes or terminations outlined in this policy.

8. ROLES AND RESPONSIBILITIES.

This section defines the roles and responsibilities for implementing data management.

a. The Chief Digital & Information Officer (CIO). CIO shall:

1) delegate data management implementation to the Chief Data and Artificial Intelligence Officer (CDAIO), or their representative;
2) ensure compliance with Federal regulations and the FISMA information technology security program implementation requirements;
3) ensure data is integrated with DOT strategic and operational planning;
4) provide resources to administer DOT data management activities;
5) ensure compliance with this policy.

b. The Chief Data and Artificial Intelligence Officer (CDAIO). CDAIO shall:

1) represent DOT on the Federal Chief Data Officer (CDO) Council and promote standards enumerated by the Council;
2) chair the DOT Data Governance Board;
3) manage data technology investments;
4) direct DOT data management policy, in coordination with the Office of the Assistant Secretary for Transportation Policy;
5) provide data and AI-enabling tools and services to the Department;
6) monitor and evaluate accuracy, effectiveness, objectivity, and usefulness of data and data solutions;
7) manage the public Enterprise Data Inventory in collaboration with Components;
8) issue and update, as appropriate, standards of quality for data;
9) direct or appoint representative(s) from Components to maintain feedback mechanisms for DOT personnel;
10) direct or appoint representative(s) from Components to maintain feedback mechanisms for the public and other stakeholders;
11) coordinate with Components to ensure a point of contact is designated to assist and respond to customer inquiries about data;
12) collaborate with Components to engage private and non-profit sector entrepreneurs and innovators to encourage and facilitate the use of data;
13) serve as the DOT representative to the Federal Geographic Data Committee (FGDC) Executive Committee and develop implementation guidance on geospatial data standards and policy;

14) promote the use of FGDC data standards, FGDC Content Standards for Digital Geospatial Metadata, and other appropriate standards, including documenting geospatial data with the relevant metadata and making metadata available;
15) coordinate and work in partnership with the following entities to collect, integrate, maintain, disseminate, and preserve geospatial data and information, building upon local data efficiently and cost-effectively:

    a) DOT Components,
    b) International, Federal, State, territorial, and Tribal government agencies,
    c) Academia, and
    d) Private Sector;

16) support emergency response activities requiring geospatial data;
17) retain and coordinate all agreements regarding use of geospatial data;
18) ensure compliance with the Geospatial Data Act and other requirements, regulations, and initiatives for geospatial data;
19) direct data upskilling activities for DOT personnel;
20) collaborate with Components, Chief Information Security Officer (CISO), and Office of the General Counsel (OGC) to facilitate compliance with this policy; and
21) conduct annual audits of this policy.

c. The Chief Information Security Officer (CISO). CISO shall:

1) implement the requirements of this policy with respect to cybersecurity principles;
2) provide strategic data security and zero trust architecture leadership; and
3) enforce data management policy compliance with applicable law, regulations, and policies in coordination with CDAIO and OGC.

d. The Senior Agency Official for Privacy (SAOP). SAOP shall:

1) implement the requirements of this policy with respect to privacy, civil rights, and civil liberties principles;
2) act as the authority for privacy compliance for data;
3) consult with the Departmental Office of Civil Rights on matters related to civil rights and civil liberties;
4) identify privacy, civil rights, and civil liberties risks to individuals and direct required mitigation efforts; and
5) collaborate with Components and CISO to ensure privacy by design throughout the data lifecycle.

e. The Senior Agency Official for Records Management (SAORM). SAORM shall:

1) implement the requirements of this policy, as they pertain to records management throughout the records lifecycle; and
2) provide strategic records management leadership for data, including assisting Components in determining retention requirements for records.

f. The Assistant Secretary for Research and Technology (OST-R), Operating Administration Chief Scientific Officer, or equivalent. OST-R and equivalents will:

1) implement the requirements of this policy and the DOT Scientific Integrity Policy, as they pertain to scientific research and scientific and technical data, including scientific collections conducted by DOT personnel;
2) ensure DOT research personnel comply with this policy;
3) collaborate with CDAIO to keep the Enterprise Use Case Inventory updated; and
4) promote the deposit of scientific and technical data and information in publicly accessible databases, including the National Transportation Library.

g. The Director of the Bureau of Transportation Statistics (BTS) or Component Chief Statisticians (CCS). BTS or CCS shall:

1) coordinate with CDAIO and Components to improve the coordination of data collection efforts within DOT and with other Federal agencies and entities; and
2) evaluate statistical programs for their use of reliable data sources and sound analytical techniques—including reproducibility standards—in consultation with relevant scientific and technical communities.

h. The Senior Procurement Executive (SPE).[6] SPE shall:

1) promote the appropriate use of required data rights clauses and terms in all applicable contracts and financial assistance agreements;
2) ensure Chiefs of Contracting Offices (COCOs) enforce the requirements of data rights clauses and terms; and
3) procure data according to Federal directives.

i. The Office of the General Counsel (OGC). OGC shall:

1) provide legal advice on compliance with this Order, consistent with applicable laws, regulations, and Executive Orders;
2) provide legal advice regarding the data rights and intellectual property issues that arise in the implementation of this policy; and
3) enforce data management policy compliance with applicable law, regulations, and policies in coordination with CDAIO and CISO.

j. The Component Chief Data Office (CCDO) or the Administrator's Representative. CCDO or the Administrator's Representative shall:

1) keep the Enterprise Data Inventory updated;
2) participate in DOT data management forums, thereby representing Component

---

[6] The Federal Aviation Administration (FAA), with its statutory independent procurement authority, is not subject to SPE authority under this section. FAA's head of contracting activity or equivalent shall ensure that data rights provisions consistent with the principles of this Order are incorporated into contracts and agreements in accordance with the FAA Acquisition Management System (AMS) and applicable FAA policies.

interests;
3) collaborate with CDAIO to comply with Information Quality Guidelines; and
4) fulfill DOT personnel upskilling activities directed by CDAIO.

k. The Component Chiefs of Contracting Offices (COCOs). COCOs shall:

1) ensure the appropriate use of data, when used in contracts and financial assistance agreements; and
2) enforce the requirements of data rights clauses and terms in collaboration with SPE.

l. The Component Chief Counsel (CCC). CCC shall:

1) provide legal advice on the Component's compliance with this policy, consistent with applicable laws, throughout the development of data;
2) consult with OGC on intellectual property and other legal issues that arise in the implementation of this policy; and
3) communicate non-compliance of data management policy to CDAIO.

9. COMPLIANCE.

DOT Components will comply with and support the implementation of this policy. This includes, but is not limited to, compliance with Federal policies, standards, and procedures.

10. WAIVERS.

Compliance with this policy is mandatory. Components may request that CDAIO grant a waiver of compliance, based on a compelling business reason. In addition to an explanation of the waiver being sought, the Component will provide DOT CDAIO:

1) Justification;
2) What measures have been implemented to ensure that data management and open data principles have been considered;
3) Waiver period; and
4) Milestones for achieving compliance.

The CDAIO will review the waiver request and provide a decision in writing; any denial of a waiver request must provide a justification for the denial.

11. EFFECTIVE DATE. This Order is effective, JUNE 23, 2026.

Sean P. Duffy

APPENDIX A:

a. Legislation

1) 49 CFR part 806, National Security Information Policy and Guidelines, Implementing Regulations.
2) 49 CFR part 1520, Protection of Sensitive Security Information.
3) 48 CFR subpart 4.19, Basic Safeguarding of Covered Contractor Information Systems.
4) 5 CFR part 1321.2. Dissemination Definitions.
5) 6 CFR part 7. Classified National Security Information.
6) 91 FR 4102, Indian Entities Recognized by and Eligible to Receive Services from the United States Bureau of Indian Affairs.
7) Government Service Delivery Improvement Act, Pub. L. No. 118-231, January 4, 2025.
8) 17 U.S.C. § 105, Subject matter of copyright: United States Government works. December 23, 2024.
9) 49 U.S.C. § 106(f)(2), Federal Aviation Administration, January 3, 2024.
10) 49 U.S.C. § 40110, Federal Aviation Administration General procurement authority. January 3, 2024.
11) 44 U.S.C. § 3502, Federal Information Policy, January 3, 2022.
12) 44 U.S.C. § 3301-3315, Disposal of Records, January 3, 2022.
13) National Artificial Intelligence Initiative Act, Pub. L. No. 116–283, March 12, 2020.
14) OPEN Government Data Act, Pub. L. No. 115-435, January 14, 2019.
15) 44 U.S.C. § 3520, Chief Data Officers, January 14, 2019.
16) Geospatial Data Act of 2018, Pub. L. No. 115-254, October 5, 2018.
17) Freedom of Information Act (FOIA) Improvement Act, 49 U.S.C. § 552.
18) 49 U.S.C. § 322, Department of Transportation Operating Administrations, April 5, 2016.
19) Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, December 18, 2014.
20) 44 U.S.C. § 3552(b)(6), Coordination of Federal Information Policy, Information Security, December 18, 2014.
21) 49 U.S.C. §§ 6301-6314, Bureau of Transportation Statistics, January 17, 2014.
22) 44 U.S.C. § 2901–2912, Records Management by the Archivist of the United States, January 3, 2012.
23) 72 FR 33362, Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002, June 15, 2007.
24) 10 U.S.C. § 948 (a)(2), Classified National Security Information, October 28, 2009.
25) E-Government Act of 2002, Pub. L. No. 107–347, December 2002.
26) Information Quality Assurance Act, Pub. L. No. 106–554, Sec. 515, December 2000.
27) National Technology and Advancement Act, Pub. L. No. 104–113, March 7, 1996.
28) 18 U.S.C. § 798 Disclosure of Classified Information, October 11, 1996.
29) Paperwork Reduction Act of 1995, Pub. L. 104-13, May 22, 1995.
30) Privacy Act of 1974, 5 U.S.C. § 552a.
31) Rehabilitation Act of 1973, Pub. L. No. 93-112, September 26, 1973.

32) 44 U.S.C. § 2101–2120, National Archives and Records Administration, October 22, 1968.
33) 44 U.S.C. § 3301, Federal Records Act of 1950.

b. National Policy, Directives and Memorandums

1) Executive Order 14409, Promoting Advanced Artificial Intelligence Innovation and Security, June 2, 2026.
2) Executive Order 14365, Ensuring a National Policy Framework for Artificial Intelligence, December 16, 2025.
3) OMB Memorandum M-26-04, Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles, December 11, 2025.
4) OMB Memorandum M-26-03, President's Management Agenda. December 8, 2025.
5) Federal Acquisition Regulation Subpart 27.4, Rights in Data and Copyrights, October 1, 2025.
6) Executive Order 14338, Improving Our Nation Through Better Design, August 26, 2025.
7) Executive Order 14319, Preventing Woke AI in the Federal Government, July 23, 2025.
8) OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, April 3, 2025.
9) Executive Order 14303, Restoring Gold Standard Science, March 23, 2025.
10) Executive Order 14243, Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, March 20, 2025.
11) Executive Order 14179, Removing Barriers to American Leadership in AI, January 23, 2025.
12) OMB Memorandum M-25-07, Broadening Public Participation and Community Engagement with the Federal Government, January 15, 2025.
13) OMB Memorandum M-25-06, Re-establishing the Chief Data Officer Council, January 15, 2025.
14) OMB Memorandum M-25-05, Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance, January 15, 2025.
15) OMB Circular A-16 and Supplemental Guidance, Coordination of Geographic Information and Related Spatial Data Activities (as amended), July 3, 2024.
16) Executive Order 14117, Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, February 28, 2024.
17) OMB Memorandum M-23-22, Delivering a Digital-First Public Experience, September 22, 2023.
18) Federal Data Strategy: Data Governance Playbook, July 1, 2020.
19) OMB Memorandum M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance, July 10, 2019.
20) OMB Memorandum M-19-18, Federal Data Strategy: A Framework for Consistency, June 4, 2019.
21) OMB Memorandum M-19-15, Improving Implementation of the Information Quality

Act, April 24, 2019.

22) OMB Memorandum M-17-12. Preparing for and responding to a breach of personally identifiable information, January 3, 2017.
23) OMB Circular A-130, Management of Federal Information Resources (as amended), July 28, 2016.
24) OMB Circular A-119 Revised, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, January 27, 2016.
25) OMB Memorandum M-15-15, Improving Statistical Activities through Interagency Collaboration, July 8, 2015.
26) Statistical Policy Directive No. 1: Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units, 79 FR 71609, December 2, 2014.
27) OMB Memorandum M-14-06, Guidance for Providing and Using Administrative Data for Statistical Purposes, February 14, 2014.
28) Executive Order 13642, Making Open and Machine-Readable the New Default for Government Information, May 9, 2013.
29) Executive Order 13556, Controlled Unclassified Information, November 4, 2010.

c. DOT Policies and Guidelines

1) DOT AI Strategy, October 3, 2025, or later version.
2) Class Deviation No. 2026-06 from the Federal Acquisition Regulation for FAR Part 27 in Support of Executive Order 14275 on Restoring Common Sense to Federal Procurement, October 1, 2025, or later revision.
3) DOT Open Data Plan, August 13, 2025, or later revision.
4) Scientific Integrity Policy of the United States Department of Transportation, January 24, 2024, or later revision.
5) FAA Order 1370.121B, FAA Information Security and Privacy Policy, April 25, 2022, or later revision.
6) DOT Order 1371.1, Data Trust Policy, Guidelines, and Principles, January 15, 2021, or later version.
7) DOT Information Dissemination Quality Guidelines, October 31, 2019, or later version.
8) DOT Order 1351.28, Records Management Policy, August 16, 2016, or later version.
9) DOT Order 1351.18, Privacy Risk Management, September 20, 2014, or later version.
10) DOT Order 1351.58, Privacy Policy for Information Sharing Environment, June 5, 2012, or later version.
11) DOT Order 1351.37, Cybersecurity Policy, June 21, 2011, or later version.
12) DOT Order 1351.19, PII Breach Notification Controls, May 14, 2009, or later revision.
13) Federal Aviation Administration Order 1600.75, Protecting Sensitive Unclassified Information (SUI), February 1, 2005, or later revision.

d. Other Relevant References

1) National Institute of Standards and Technology (NIST), Human-Centered AI, April 23, 2024.
2) NIST Special Publication (SP) 800-47, Rev. 1., Managing the Security of Information Exchanges, July 20, 2021.
3) NIST, SP 800-209, Security Guidelines for Storage Infrastructure, October 26, 2020.
4) NIST, AI Use Case Taxonomy, March 26, 2024.
5) Committee on National Security Systems, (CNSS) 4009 Glossary, March 2, 2022.
6) NIST PUB 140-3, Federal Information Processing Standards, March 22, 2019.
7) NIST SP 800-175A, Guidelines for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, August 23, 2016.

APPENDIX B: DEFINITIONS

a. Accessibility: Information technology products or services that are in full compliance with the standards of Section 508 (Rehabilitation Act of 1973).

b. Artificial intelligence (AI): A machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to:

    1) perceive real and virtual environments;
    2) abstract such perceptions into models through analysis in an automated manner; and
    3) use model inference to formulate options for information or action. (15 U.S.C. § 9401.15 (3)).

c. Data: Recorded information, regardless of the form or media on which it is recorded. Subcategories include, but are not limited to, geospatial, unstructured, and structured data (Open Government Data Act, OMB Circular A-130, Geospatial Data Act, and OMB M-25-05).

d. Data asset: A collection of data elements or data sets that may be grouped together (44 U.S.C. § 3502).

e. Data governance: A set of processes that ensure that data assets are formally managed throughout the enterprise (CNSS 4009 Glossary).

f. Data encryption: The process of a confidentiality mode that transforms usable data into an unreadable form (NIST SP 800-175A).

g. Data exchange: The access to or the transfer of data outside of system authorization boundaries to accomplish a mission or business function (NIST Special Publication 800-47).

h. Data storage management: All activities geared toward ensuring reliability, resilience, performance, and security of storage resources using management tools and processes (NIST SP 800-209).

i. Data trust: a tool for sharing sensitive data among trust members for advancing safety or other public benefits when there might otherwise be strong disincentives or significant barriers to sharing (DOT Order 1371.1).

j. Dissemination: The government-initiated distribution of information to a non-government entity, including the public (5 CFR 1321.2).

k. DOT personnel: All DOT Federal employees and contractors.

l. Enterprise data inventory: The publicly available comprehensive listing of data and data assets at DOT (Open Government Data Act).

m. Human-centered AI: Development of AI systems that prioritize human needs, values, and capabilities at the core of their design and operation. Human-centered AI is where AI is used to support inherently human processes, AI augments the mission in an iterative fashion, and personnel are held accountable for AI-assisted outcomes (NIST AI Use Taxonomy).

n. Identity and access management: Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users (NIST Special Publication 800-175A).

o. Information exchange: The access to or the transfer of data outside of system authorization boundaries to accomplish a mission or business function (NIST Special Publication 800-47, Revision 1).

p. Metadata: Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher, or responsible party, contact information, method of collection, and other descriptions (Open Government Data Act).

q. Memorandum of Understanding or Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In the context of this policy, a MOU/A defines the responsibilities of two or more organizations for securely sharing safeguarded, sensitive data and information (NIST Special Publication 800-47).

r. Open License: A legal guarantee applied to a public data asset that is made available at no cost to the public and with no restrictions on the copying, publishing, distributing, transmitting, citing, or adapting thereof (Open Government Data Act).

s. Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (Privacy Act).

t. Sensitive Personally Identifiable Information (Sensitive PII or SPII): A subset of PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

The following PII is always *(de facto)* sensitive, with or without any associated personal information, and cannot be treated as low confidentiality:

1) Social Security number (SSN);
2) Passport number;

3) Driver's license number;
4) Biometrics, such as finger or iris print, and DNA;
5) Financial account number such as credit card or bank account number; or
6) The combination of any individual identifier and date of birth, or mother's maiden name, or last four of an individual's SSN (DOT Order 1351.19).

u. Sensitive Security Information (SSI): Information obtained or developed in the conduct of security activities, including research and development, the disclosure of which Transportation Security Administration has determined would (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to the security of transportation (49 CFR part 1520).