Subject: U.S. DEPARTMENT OF TRANSPORTATION ARTIFICIAL INTELLIGENCE (AI) POLICY

1. PURPOSE

This policy establishes the U.S. Department of Transportation (DOT) policy on internal applications of AI by DOT personnel, which provides high-level directives to which DOT Operating Administrations and Secretarial Offices (herein, "Components")[5] must adhere to throughout the AI lifecycle.

2. BACKGROUND

DOT uses AI in support of its work to advance transportation safety and improve operational efficiency. This policy enables a structured and thoughtful approach for the DOT acquisition, management, and adoption of AI. This policy can remove barriers to AI innovation and increase public trust in DOT use of AI through transparency, accountability, and effectiveness.

DOT has a default posture of "Use AI when appropriate," meaning AI activities are permissible to the greatest extent possible, practicable, and consistent with law. DOT personnel should determine whether the business challenge requires AI or another approach.

DOT is committed to human-centered AI. Human-centered AI refers to the development of AI that prioritizes human needs, values, and capabilities.

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

3. REFERENCES

See Appendix A.

4. DEFINITIONS

See Appendix B.

5. SCOPE

This policy applies to the use by DOT personnel of AI implemented on DOT information systems.

---

[5] The Office of Inspector General (OIG) is not a Component as defined in this policy but will issue internal policies consistent with this policy and work with the DOT OCIO/CDAIO when consistent with OIG independence.

This policy applies to AI implementations at DOT that predate this policy. Components will have up to six months to submit a list of AI activities that predate this policy to the Chief Data and Artificial Intelligence Officer (CDAIO) and will review those activities to bring them into compliance with this policy.

This policy applies to all DOT personnel and all Components.

This policy does not apply to AI when it is being used as a component of a National Security System.[6]

This policy does not apply to the use of AI to carry out basic research or applied research, except where the purpose of such research is to develop AI applications for agency use.[7]

This policy does not apply to AI products, services, or systems that DOT-regulated entities or funding recipients use or develop.

In addition to the requirements stated herein, AI must adhere to existing Federal laws, DOT policies, and implementation guidance.

6. POLICY

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

a. AI lifecycle practices.

Components should apply five distinct phases (Design, Development, Deployment, Monitoring and Evaluation, and Disposal of or Transfer) during the iterative AI lifecycle. Human oversight will be incorporated during each phase. When AI is used for purposes of a final DOT action document, the results shall be reviewed and validated by a qualified and responsible employee of the Department. Components may incorporate additional principles, practices, or activities consistent with this policy.

1) Design

a) DOT will determine whether AI is needed to solve a business challenge.
b) DOT will design or select AI to meet its needs.
c) DOT will protect federal information.
d) DOT will plan AI for maximum long-term value and reusability.

2) Development

a) DOT will involve stakeholders early and often before AI is deployed.

---

[6] AI innovation and risk for National Security Systems must be managed appropriately, but these systems are governed through other policies. Agencies should reference existing guidelines in place, such as the Department of War's (DoW) Responsible Artificial Intelligence Strategy and Implementation Pathway and the Office of the Director of National Intelligence's Principles of Artificial Intelligence Ethics for the Intelligence Community, as well as policies governing specific high-risk national security applications of AI, such as DoW Directive 3000.09, Autonomy in Weapon Systems, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

[7] In the context of AI, the terms "basic research" and "applied research" are defined in OMB M-25-21.

b) DOT will adhere to existing information quality standards, data management, data governance, and AI governance policies and guidelines.
c) DOT will procure AI according to federal directives.

3) Deployment

a) DOT will ensure DOT personnel use only authorized AI.
b) DOT will enforce Acceptable Rules of Behavior.

4) Monitoring and Evaluation

a) DOT will develop processes to prevent, monitor, and minimize AI risk to the greatest extent practicable.
b) DOT will develop processes for monitoring and evaluating accuracy, effectiveness, objectivity, and usefulness.

5) Dispose of or Transfer

a) DOT will classify records based on the business function they serve, rather than whether they are AI generated or used in AI according to federal directives; and shall retain those records in an appropriate designated recordkeeping system.
b) DOT will retain generative AI prompts and outputs for 7 days, after which they will be automatically destroyed or purged.
c) DOT will use approved recordkeeping repositories. AI tools and platforms are not approved recordkeeping repositories. A record generated by or used in DOT-approved AI must be captured and transferred from the AI platform into the appropriate designated recordkeeping system.
d) DOT will adhere to and comply with the National Archives and Records Administration (NARA) approved retention schedules for records generated by AI or used in AI.
e) DOT will retire AI models or solutions that are no longer suitable or viable for their intended purpose according to federal directives.

b. AI risk management.

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

1) DOT will consider AI 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 AI to minimize negative impacts.

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

7. ROLES AND RESPONSIBILITIES

This section describes the roles and responsibilities for implementing AI.

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

1) delegate AI implementation to the Chief Data and Artificial Intelligence Officer (CDAIO), or their representative;
2) ensure compliance with federal regulations and the Federal Information Security Modernization Act (FISMA) information technology security program implementation requirements;
3) ensure AI is integrated with DOT strategic and operational planning;
4) provide resources to administer DOT AI activities;
5) collaborate with the Chief Data and Artificial Intelligence Office (CDAIO) to review existing AI solutions and their technical capabilities before procuring new AI solutions;
6) review and approve required privacy documentation before AI is acquired;
7) ensure information technology systems provide AI capabilities; and
8) 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) vice-chair proceedings of the DOT AI Governance Board[8];
3) manage AI technology investments;
4) direct DOT AI policy, in coordination with the Office of the Assistant Secretary for Transportation Policy;
5) communicate the value of AI;
6) direct decisions that promote human-centered AI;
7) coordinate with CIO to review existing AI and their technical capabilities before procuring new AI;
8) establish AI risk assessment and mitigation processes to prevent, monitor, and minimize risks to the greatest extent practicable;
9) monitor and evaluate accuracy, effectiveness, objectivity, and usefulness of AI models and solutions;
10) manage the public AI Use Case Inventory in collaboration with Components;

[8] The DOT NETT Council has been designated as the agency AI Governance Board. CDAIO is responsible for bringing AI governance topics to the NETT Council.

11) review and approve new and high-impact AI use cases in collaboration with the Senior Agency Official for Privacy (SAOP), Office of General Counsel (OGC), Components, and DOT Chief Information Security Officer (CISO), except for FAA use cases. For FAA use cases, CDAIO will delegate approval authority in accordance with independent FAA statutory authorities;
12) issue and update, as appropriate, standards of quality for underlying data and models;
13) direct or appoint representative(s) from Components to maintain feedback mechanisms for DOT personnel;
14) direct or appoint representative(s) from Components to maintain feedback mechanisms for the public and other stakeholders;
15) coordinate with Components to ensure that a point of contact is designated to assist and respond to customer inquiries about AI;
16) collaborate with Components to engage private and nonprofit sector entrepreneurs and innovators to encourage and facilitate the use of AI;
17) ensure compliance with the Geospatial Data Act and other requirements, regulations, and initiatives for geospatial AI;
18) direct AI upskilling activities for DOT personnel;
19) collaborate with Components to facilitate compliance with this policy;
20) enforce AI policy compliance with applicable law, regulations, and policies in coordination with CISO and OGC; 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 AI cybersecurity leadership;
3) review AI Use Case Inventory waivers in consultation with CDAIO, OGC, and SAOP;
4) enforce Acceptable Use Rules of Behavior in collaboration with CDAIO, OGC, and SAOP;
5) oversee operational protection and incident response for the use of AI as described in DOT cybersecurity policy or guidelines; and
6) enforce AI 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 AI;
3) consult with the DOT Office of Civil Rights on matters related to civil rights and civil liberties;
4) review and approve required privacy documentation before AI is acquired in collaboration with CIO;
5) identify privacy, civil rights, and civil liberties risks to individuals and direct

required mitigation efforts;
6) collaborate with Components and CISO to ensure privacy by design throughout the AI lifecycle; and
7) review AI use case waivers in consultation with CDAIO, CISO, and OGC.

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;
2) provide strategic records management leadership for AI records, including assisting Components in determining retention requirements for AI records; and
3) update AI upskilling activities for DOT personnel to include records management topics.

f. The Assistant Secretary for Research and Technology (OST-R), Operating Administration Chief Scientist, or equivalent. OST-R and OA Chief Scientist shall:

1) implement the requirements of this 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) evaluate AI feasibility to the greatest extent practicable; and
4) collaborate with CDAIO to keep the AI Use Case Inventory updated.

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

1) coordinate with CDAIO, CISO, SAOP, or others to implement AI; and
2) evaluate Component statistical programs for their use of AI, including reproducibility standards, in consultation with relevant scientific and technical communities.

h. The Senior Procurement Executive (SPE)[9]. SPE shall:

1) ensure the appropriate acquisition of AI solutions in contracts;
2) prevent the procurement of overlapping AI capabilities in collaboration with CDAIO and CIO;
3) ensure Chiefs of Contracting Offices (COCOs) enforce the requirements of data rights clauses and terms; and
4) procure AI according to Federal directives.

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

[9] The Federal Aviation Administration (FAA), with its statutory independent procurement authority, is not subject to SPE authority under this section. The 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.

1) provide legal advice on compliance with this policy, 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;
3) provide legal advice regarding the use of AI in personnel matters, to include, ensuring that any use of AI in matters affecting personnel actions, equal employment opportunity complaints, whistleblower disclosures, or labor relations complies with due-process requirements, evidentiary standards, and applicable case law, and that AI outputs are not treated as independent factual findings or credibility determinations;
4) review AI Use Case Inventory waivers in collaboration with CDAIO, CISO, and SAOP; and
5) enforce AI policy compliance with applicable law, regulations, and policies in coordination with CDAIO, OGC, and CISO.

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

1) determine whether AI is the appropriate approach to meet the mission need in coordination with Component leadership, COCO or OGC;
2) review approved use cases before submitting new requests to CDAIO;
3) designate a person or office that has the authority for ensuring Component compliance with this policy;
4) disclose AI that predates this policy to CDAIO within six months of the enactment date;
5) ensure AI that predates this policy complies with this policy as soon as practicable;
6) collaborate with CDAIO to keep the AI Use Case Inventory updated;
7) apply human-centered AI principles throughout the AI lifecycle;
8) ensure AI is continuously monitored and retired or replaced when necessary;
9) implement AI with the most transparency practicable, as permitted by law and other requirements;
10) participate in DOT AI forums, thereby representing Component interests;
11) collaborate with Components to apply this policy;
12) enforce AI labeling rules to the greatest extent practicable; and
13) fulfill DOT personnel upskilling activities directed by CDAIO.

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

1) ensure the use of AI is appropriate when used in contracts and financial assistance agreements.
2) enforce the requirements of AI terms in contracts; and
3) 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 AI;
2) provide advice to the Component regarding public release disclosure assessments;
3) consult with OGC on intellectual property and other issues that arise in the implementation of this policy; and
4) prior to deployment of any AI within the Component, review AI compliance with applicable law, regulations, and policies; and
5) communicate non-compliance of AI policy to CDAIO.

8. DATES

This policy is effective as of the date it is signed.

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.

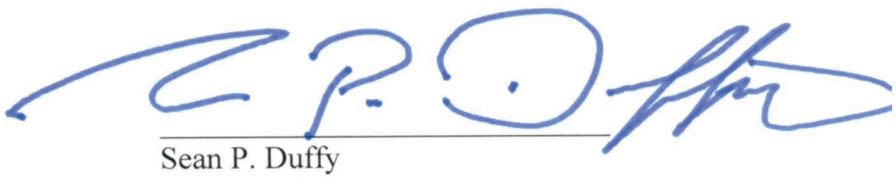
10. WAIVERS

Compliance with this policy is mandatory. Components may request a waiver of compliance for a use case to be included in the AI Use Case inventory, 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 AI management principles have been considered;
3) Waiver period; and
4) Milestones for achieving compliance.

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



Sean P. Duffy

APPENDIX A:

a. **Legislation and Regulation**

1) 49 CFR Part 1520, Protection of Sensitive Security Information.
2) 49 CFR Part 806, National Security Information Policy and Guidelines, Implementing Regulations.
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) 49 U.S.C. § 106(f)(2), Federal Aviation Administration. January 3, 2024.
9) 49 U.S.C. § 40110, Federal Aviation Administration General procurement authority. January 3, 2024.
10) 44 U.S.C. §3502, Federal Information Policy. January 3, 2022.
11) 44 U.S.C. § 3301-3315, Disposal of Records. January 3, 2022.
12) Identifying Outputs of Generative Adversarial Networks Act, Pub. L. No. 116–258. December 23, 2020.
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) Geospatial Data Act, Pub. L. No. 115-254, Subtitle F. October 5, 2018.
16) Freedom of Information Act (FOIA) Improvement Act, 49 U.S.C. § 552.
17) 49 U.S.C. § 322, Department of Transportation Operating Administrations. April 5, 2016.
18) Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq*. December 18, 2014.
19) 44 U.S.C. § 3552(b)(6), Coordination of Federal Information Policy, Information Security. December 18, 2014.
20) 44 U.S.C. § 2901–2912, Records Management by the Archivist of the United States. January 3, 2012.
21) 10 U.S.C. § 948 (a)(2), Classified National Security Information. October 28, 2009.
22) Information Quality Act, Pub. L. No. 106–554, Sec. 515. December 2000.
23) National Technology and Advancement Act, Pub. L. No. 104–113. March 7, 1996.
24) 18 U.S.C. § 798, Disclosure of Classified Information. October 11, 1996.
25) 5 U.S.C. § 552a, The Privacy Act of 1974.
26) 44 U.S.C. § 3301, Federal Records Act of 1950.
27) 44 U.S.C. § 2101–2120, National Archives and Records Administration. October 22, 1968.

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) Executive Order 14363, Launching the Genesis Mission. November 24, 2025.
6) Federal Acquisition Regulation Subpart 27.4, Rights in Data and Copyrights. October 1, 2025, or later revision.
7) OMB Memorandum M-25-34, NSTM-2, Fiscal Year (FY) 2027 Administration Research and Development Budget Priorities. September 23, 2025.
8) Executive Order 14338, Improving Our Nation Through Better Design. August 26, 2025.
9) White House AI Action Plan. July 23, 2025.
10) Executive Order 14319, Preventing Woke AI in the Federal Government. July 23, 2025.
11) Executive Order 14318, Accelerating Federal Permitting of Data Center Infrastructure. July 23, 2025.
12) OMB Guidance on 2025 Agency Artificial Intelligence Reporting. June 27, 2025.
13) Executive Order 14307, Unleashing American Drone Dominance. June 6, 2025.
14) Executive Order 14275, Restoring Common Sense to Federal Procurement. April 15, 2025.
15) OMB Memorandum M-25-22, Driving Efficient Acquisition of Artificial Intelligence in Government. April 3, 2025.
16) OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust. April 3, 2025.
17) Executive Order 14303, Restoring Gold Standard Science. March 23, 2025.
18) Executive Order 14243, Stopping Waste, Fraud, and Abuse by Eliminating Information Silos. March 20, 2025.
19) Executive Order 14179, Removing Barriers to American Leadership in AI. January 23, 2025.
20) 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.
21) OMB Memorandum M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements. January 15, 2025.
22) Executive Order 14141, Advancing U.S. Leadership in AI Infrastructure. January 14, 2025.

23) National Spatial Data Infrastructure Strategic Plan 2025 – 2035: Building the Geospatial Future Together. October 16, 2024.
24) OMB Circular A-16 and Supplemental Guidance, Coordination of Geographic Information and Related Spatial Data Activities (as amended). July 3, 2024.
25) 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.
26) OMB Memorandum M-23-22, Delivering a Digital–First Public Experience. September 22, 2023.
27) OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. January 26, 2022.
28) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information. January 3, 2017.
29) OMB Circular A-130, Management of Federal Information Resources (as amended). July 28, 2016.
30) Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002, 72 FR 33361. June 15, 2007.

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) DOT Compliance Plan for OMB Memorandum M-24-10. September 24, 2024, or later revision.
5) ITIM 2024-001. DOT Acceptable Use Rules of Behavior. April 3, 2024, or later revision.
6) Scientific Integrity Policy of the United States Department of Transportation. January 24, 2024, or later revision.
7) FAA Order 1370.121B, FAA Information Security and Privacy Policy. April 25, 2022, or later revision.
8) DOT Order 1371.1, Data Trust Policy, Guidelines, and Principles. January 15, 2021, or later version.
9) DOT Information Dissemination Quality Guidelines. October 31, 2019, or later version.
10) DOT Order 1120.34, U.S. Department of Transportation's Non-Traditional and Emerging Transportation Technology Council. December 11, 2018, or later version.
11) DOT Order 1351.34, Data Management Policy. July 13, 2017, or later version.
12) DOT Order 1351.28, Records Management Policy. August 16, 2016, or later version.
13) DOT Order 1351.18, Privacy Risk Management. September 20, 2014, or later version.

14) DOT Order 1351.58, Privacy Policy for Information Sharing Environment. June 5, 2012, or later version.
15) DOT Order 1351.37, Cybersecurity Policy. June 21, 2011, or later version.
16) Federal Aviation Administration Order 1600.75, Protecting Sensitive Unclassified Information (SUI). February 1, 2005, or later revision.

d. **Other Relevant References**

1) General Services Administration, IT Modernization Centers of Excellence, AI Guide for Development. January 13, 2026.
2) National Institute of Standards and Technology, Secure Software Development Practices for Generative AI, and Dual-Use Foundation Models. Special Publication 800-218. July 26, 2024.
3) National Institute of Standards and Technology, Human-Centered AI. April 23, 2024.
4) National Institute of Standards and Technology, AI Risk Management Framework. January 2023.
5) National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, September 23, 2020.
6) National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems FIPS Publication 199. February 1, 2004.

APPENDIX B: DEFINITIONS

a. 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))

b. AI use case: An AI use case refers to the specific scenario in which AI is designed, developed, procured, or used to advance the execution of agencies' missions and their delivery of programs and services, enhance decision making, or provide the public with a particular benefit. (OMB Guidance on 2025 Agency Artificial Intelligence Reporting)

c. AI Use Case Inventory: A public listing of DOT use cases posted on the agency's website. (OMB M-25-21) If AI is used or developed by DOT personnel for State DOT, Metropolitan Planning Organizations, or other agencies, it should be listed in the DOT Use Case Inventory.

d. AI risk: Risk refers to the composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event. The impacts, or consequences, of AI systems can be positive, negative, or both and can result in opportunities or threats. When considering the negative impact of a potential event, risk is a function of 1) the negative impact, or magnitude of harm, that would arise if the circumstance or event occurs and 2) the likelihood of occurrence. (Adapted from: OMB Circular A-130) Negative impact or harm can be experienced by individuals, groups, communities, organizations, society, the environment, and the planet. (NIST AI Risk Management Framework)

e. AI lifecycle: The iterative process of moving from a business problem to an AI solution that solves that problem. (GSA IT Modernization Centers of Excellence) DOT has added a Disposition or Transfer step aligning with Records Management standards.

f. Classified information: Any material or information determined under Executive Order, statute, or regulation to require protection against unauthorized disclosure to safeguard national security. (10 U.S.C. § 948a (2))

g. Components: DOT Operating Administrations (OAs) and Secretarial Offices. (49 CFR Part 1D)

h. Data: Recorded information, regardless of the form or media on which it is recorded. For the purposes of this policy, data refers to information retained as official records or evidence in accordance with applicable records schedules, privacy requirements, and data governance policies. Types of data 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)

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

j. Generative AI: The class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content. (NIST Special Publication 800-218)

k. High-Impact AI: AI output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on:

   1) An individual or entity's civil rights, civil liberties, or privacy;
   2) An individual or entity's access to education, housing, insurance, credit, employment, and other programs. An individual or entity's access to critical government resources or services. DOT considers hiring, non-selection, promotion, performance evaluation, discipline, adverse actions, suitability, fitness-for-duty, reasonable accommodation, labor-relations matters, or whistleblower reprisal determinations for DOT personnel high-impact AI;
   3) Human health and safety;
   4) Critical infrastructure or public safety;
   5) Strategic assets or resources, including high-value property such as airports, physical inventory under the purview of FAA; and
   6) Information marked as sensitive or classified by the Federal Government. (OMB M-25-21)

l. 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 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)

m. Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. (NIST FIPS 199)

n. Information, Federal: information collected or maintained on behalf of each agency. (NIST FIPS 199)

o. Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C. § 3502(8))

p. 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; OMB M-17-12)

q. 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)

r. 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)

s. Sensitive Unclassified Information (SUI): SUI is unclassified information – in any form including print, electronic, visual, or aural forms - that we must protect from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act (FOIA). (FAA Order 1370.121B and FAA Order 1600.75)

t. Trustworthy and Responsible AI: AI built on a framework that includes the characteristics of validity, reliability, safety, security, resiliency, accountability, transparency, interpretability, privacy, and fairness with mitigation of harmful bias. (NIST Risk Management Framework)