



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.24.1

FEBRUARY 10, 2026

EFFECTIVE DATE

(02-10-2026)

PURPOSE

- (1) This transmits new IRM 10.24.1, Artificial Intelligence, IRS Policy for Artificial Intelligence (AI) Governance.

MATERIAL CHANGES

- (1) IRM 10.24.1 establishes requirements for IRS development, implementation, and use of AI, considering recent Presidential Executive Orders (EOs) and new memoranda and instructions from the Office of Management and Budget (OMB).

EFFECT ON OTHER DOCUMENTS

This IRM replaces the Interim Guidance Memorandum RAAS-10-0325-0001, Interim Policy for AI Governance, issued on March 11, 2025.

AUDIENCE

IRM 10.24.1, IRS Policy for Artificial Intelligence (AI) Governance, will be distributed to all personnel responsible for developing, procuring, using, and monitoring AI. This policy applies to all IRS employees, contractors, and vendors.

Reza Rashidi
Chief Data and Analytics Officer
Research, Applied Analytics and Statistics (RAAS)

10.24.1

IRS Policy for Artificial Intelligence (AI) Governance

Table of Contents

10.24.1.1 Program Scope and Objectives

10.24.1.1.1 Background

10.24.1.1.2 Authority

10.24.1.1.3 Roles and Responsibilities

10.24.1.1.4 Program Management and Review

10.24.1.1.5 Program Controls

10.24.1.1.6 Terms and Acronyms

10.24.1.1.7 Related Resources

10.24.1.2 Principles for Use of AI

10.24.1.3 AI Governance

10.24.1.3.1 AI Definition

10.24.1.3.2 AI Use Case

10.24.1.4 High-Impact AI Use Cases

10.24.1.4.1 High-Impact AI Definition

10.24.1.4.2 Determination of High-Impact AI

10.24.1.4.3 Minimum Risk Management Practices for High-Impact AI

10.24.1.4.4 Requests for Waivers from High-Impact AI Minimum Risk Management Practices

10.24.1.4.5 Tracking and Reporting of Determinations, Certifications, and Waivers

10.24.1.4.6 Termination of Non-Compliant AI

10.24.1.5 AI Use Case Inventory

10.24.1.5.1 Requirements for the Inventory of AI Use Case(s)

10.24.1.5.2 Inventory Entries

10.24.1.5.3 Inventory Maintenance and Validation

10.24.1.6 AI Model and Data Inventory

10.24.1.7 Generative AI (GenAI) Policy

10.24.1.7.1 Generative AI (GenAI) Definition

10.24.1.7.2 Prohibited Uses of GenAI

10.24.1.7.3 GenAI Guidelines

10.24.1.7.4 GenAI Considerations

10.24.1.8 AI Recordkeeping Requirements

10.24.1.9 Protection of Taxpayer Rights

10.24.1.10 Privacy and Security Requirements

Exhibits

10.24.1-1 Terms and Acronyms

10.24.1-2 Related Resources

10.24.1.1
(02-10-2026)
Program Scope and Objectives

- (1) **Purpose:** The purpose of this program is to implement comprehensive IRS-wide AI governance policy to accelerate the trustworthy design, development, acquisition, and use of AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, civil liberties, and American values, consistent with applicable law and policy.
- (2) **Audience:** The provisions within this manual apply to:
 - a. All offices, businesses, operating units, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate information systems that store, process, or transmit IRS information or connect to an IRS network or system.
- (3) **Policy Owner:** Chief Data and Analytics Officer (CDAO), who also serves as the IRS Responsible AI Official (RAIO) – hereafter CDAO/RAIO.
- (4) **Program Owner:** CDAO/RAIO.
- (5) **Program Goals:** To support the trustworthy, transparent, and responsible use of AI at the IRS.

10.24.1.1.1
(02-10-2026)
Background

- (1) IRS use of AI is governed by the *Advancing American AI Act*, EOs and Office of Management and Budget (OMB) government-wide memoranda and directives, and by further direction received from the Department of the Treasury.
- (2) *EO 13859* of February 11, 2019, Maintaining American Leadership in Artificial Intelligence, outlines a policy to foster public trust and confidence in AI technologies and requires the improvement of AI model and data catalogs.
- (3) *EO 13960* of December 8, 2020, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, directs agencies to abide by nine guiding principles for government use of AI and to collect and report a comprehensive annual AI use case inventory.
- (4) *EO 14179* of January 23, 2025, Removing Barriers to American Leadership in Artificial Intelligence, tasked the OMB Director, in coordination with the Assistant to the President for Science and Technology, to publish two OMB Memoranda to guide federal government acquisition and govern the use of AI. OMB published M-25-21 (governance) and M-25-22 (acquisition) on April 3, 2025.
- (5) *EO 14319* of July 23, 2025, Preventing Woke AI in the Federal Government, describes two “Unbiased AI Principles” to guide federal agency acquisition or development of Large Language Models (LLMs), including detailed guidance in OMB M-26-04.
- (6) OMB Memorandum M-25-21 of April 3, 2025, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, provides detailed guidance for AI governance in federal agencies. M-25-21 is a central reference for this IRM.
- (7) OMB Memorandum M-25-22 of April 3, 2025, Driving Efficient Acquisition of Artificial Intelligence in Government, provides detailed guidance for federal agency acquisition of AI products and services. While M-25-22 is primarily focused on AI procurement policy and not AI governance, we include selected

references here for project teams to understand that there are requirements relating to AI procurements, and to more fully explore when developing acquisition plans.

- (8) OMB Memorandum M-26-04 of December 11, 2025, Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles, complements Executive Order 14319 and OMB Memorandum M-25-22 by providing implementation guidance to ensure that Large Language Models (LLMs) procured by the Federal Government produce reliable outputs free from harmful ideological biases or social agendas.
- (9) Treasury published the Treasury Artificial Intelligence System User Agreement on October 17, 2025, and IRS use of AI must conform to this agreement. The agreement is hosted on the *my.treasury.gov Artificial Intelligence and Large Language Learning Models* site.
- (10) Treasury published the U.S. Department of the Treasury Compliance Plan for OMB Memorandum M-25-21 in December 2025. This plan outlines special requirements for governance of Treasury-internal AI use cases, and those requirements are integrated throughout this IRM.
- (11) Treasury published the U.S. Department of the Treasury's AI Strategy for OMB Memorandum M-25-21 in December 2025. The high-level strategy aligns with OMB M-25-21 and reflects an innovation-oriented approach to AI adoption rooted in strong governance, security, and risk management.

10.24.1.1.2 (02-10-2026) Authority

- (1) *Advancing American AI Act*, See Pub. L. No. 117-263, div. G, title LXXII, subtitle B, 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 USC 11301 note).
- (2) *EO 13859*, Maintaining American Leadership in Artificial Intelligence.
- (3) *EO 13960*, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.
- (4) *EO 14179*, Removing Barriers to American Leadership in Artificial Intelligence.
- (5) *EO 14319*, Preventing Woke AI in the Federal Government.
- (6) *OMB Memorandum M-25-21*, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust.
- (7) *OMB Memorandum M-25-22*, Driving Efficient Acquisition of Artificial Intelligence in Government.
- (8) *OMB Memorandum M-26-04*, Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles.

10.24.1.1.3 (02-10-2026) Roles and Responsibilities

- (1) The **CDAO/RAIO** is tasked with overseeing the implementation of federal AI governance and assurance requirements within the IRS. This role aligns with the direction and delegated authority from the Department of the Treasury's Chief AI Officer (CAIO). The CDAO/RAIO must:
 - a. Promote agency-wide responsible AI innovation and adoption through a governance and oversight process.
 - b. Oversee IRS compliance with requirements to manage risks from the use of AI.

- c. Coordinate with accountable agency officials to ensure that the IRS's use of AI complies with applicable law and government wide guidance.
 - d. Establish, maintain, oversee, and report the agency's AI Use Case Inventory in accordance with applicable law and policy.
 - e. Ensure that custom-developed AI code and the data used to develop and test AI are appropriately inventoried, shared, and released in agency code and data repositories, in coordination with relevant officials.
 - f. Establish processes for determining, documenting, centrally tracking, monitoring, and evaluating IRS AI use cases, including independent reviews of all high-impact use cases, determinations, and waivers and the certification and oversight of high-impact AI pilot projects.
 - g. Review determinations from accountable agency officials that a presumed-high-impact AI use case is not, in fact, high-impact, and override such determinations when deemed necessary.
 - h. Establish processes to measure, monitor, and evaluate the ongoing performance and effectiveness of the agency's high-impact AI applications.
 - i. Certify high-impact AI pilot projects to proceed without one or more minimum risk management practices.
 - j. Serve as the senior advisor on AI to the Commissioner of Internal Revenue and within IRS executive decision-making forums.
 - k. Represent the IRS in, and collaborate with, coordination bodies relating to AI activities, including external forums such as AI-related councils, standard-setting bodies, relevant governance boards, or international bodies.
 - l. Advise on the transformation of the IRS's workforce into an AI-ready workforce.
 - m. Provide guidance on AI investments to the Commissioner of Internal Revenue and Chief Financial Officer related to resourcing requirements relating to AI and agency efforts to track AI spending.
- (2) **Accountable agency officials** are generally IRS leaders in executive or managerial roles - or their properly designated acting equivalents – who are trained and empowered to identify, assess, mitigate, and accept risk for one or more AI use cases, and who are accountable for the mission outcome of the AI use case(s). IRS business unit leaders may determine who is truly “accountable” for the mission outcome of the AI use case.

Accountable agency officials are also responsible for conducting and managing AI use within their business units in compliance with this IRM and other applicable policies, including IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA), to ensure their business units complete a PCLIA when required, such as for systems or projects that involve personally identifiable information (PII).

Accountable agency officials must:

- a. Ensure project team completion of all internal business unit requirements before engaging with enterprise AI use case governance, when the business unit elects to establish internal AI use case development and review processes that precede - but do not supersede or replace - service-wide AI governance.
- b. Determine, track, and record whether each AI use case – upon initiation or at any lifecycle stage thereafter – meets the OMB-provided definition of high-impact AI. If the accountable agency official identifies the use case as one that is presumed-high-impact, but determines that it is not,

in fact, high-impact, the accountable agency official must document and provide justification to the CDAO/RAIO via the CDAO AI team. All determinations must be recorded in the IRS AI Use Case Inventory. See IRM 10.24.1.4, High-Impact AI Use Cases.

- c. Document, track, and record all risk-acceptance approvals to initiate and employ AI for operational use in the IRS AI Use Case Inventory.
- d. Request and receive documented approval from the Treasury CAIO, via the CDAO/RAIO and CDAO AI team, for waiver from any high-impact AI minimum risk management practices. Waivers may only be approved based upon a system- and context-specific risk assessment declaring that fulfilling the minimum risk management practice requirement(s) would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations.
- e. Request and receive documented certification from the CDAO/RAIO via the CDAO AI team to implement high-impact AI pilot projects when the pilot would proceed without application of one or more minimum risk management practices.

(3) **The Data and Analytics Strategic Integration Board (DASIB)**, purpose, scope, membership, and additional roles are defined in IRM 1.7.1.2.1, Data and Analytics Strategic Integration Board Purpose and Scope. CDAO/RAIO is co-chair. The DASIB must:

- a. Serve as the IRS's ultimate decision-making body for final determination of high-impact AI when the accountable agency official overrides a presumption of high-impact to determine that the particular use is not, in fact, high-impact.
- b. Serve as the IRS's ultimate decision-making body for final certification of high-impact AI pilot projects to proceed without implementation of one or more high-impact AI minimum risk management practices.
- c. Review and consult with accountable agency officials on any proposal for Treasury CAIO waiver from high-impact AI minimum risk management practices.

(4) The **AI Assurance Team (AIAT)** is a cross-functional team of subject-matter experts from several business units. The AIAT must:

- a. Conduct preliminary reviews of accountable agency official requests for waiver from one or more minimum risk management practices for high-impact AI. These requests must address system-specific and context-specific risk assessment and must conclude that fulfilling one or more minimum risk management practice requirements for the particular high-impact AI use case would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. The AIAT must then advise the DASIB on the clarity, detail, and appropriateness of all requests for Treasury CAIO waiver from high-impact AI minimum risk management practices.
- b. Conduct preliminary reviews of accountable agency official requests for certification of high-impact AI pilot projects to proceed without implementation of one or more high-impact AI minimum risk management practices. The AIAT must then advise the DASIB on the clarity, detail, and appropriateness of all requests for certification for high-impact pilot projects to proceed without implementation of one or more high-impact AI minimum risk management practices.

- c. Conduct secondary reviews of accountable agency official determinations that a presumed high-impact AI use case is not, in fact, high-impact. The AIAT must then advise the DASIB of concurrence or substantive non-concurrence with the accountable agency official's determination.
- d. Conduct independent reviews of AI minimum risk management practices for high-impact AI and document the outcome of those reviews in the AI Use Case Inventory before risk acceptance by the accountable agency official.

- (5) The **CDAO AI team** supports the CDAO/RAIO in administering IRS-wide AI governance and assurance programs and processes, including management of the IRS AI Use Case Inventory, AI-related model and data inventory, inventory access controls, and providing assurance-related resources to AI project teams. Any IRS business unit or program office may contact the CDAO AI

#

quirements, and resources.

Business units and program offices may also seek support or guidance from the CDAO AI team for general introductory training, coordinating communication, and other actions related to the use of AI at the IRS. Visit the *CDAO AI Governance* site for more information.

- (6) **AI project teams and individual employees** who are responsible for the design, development, deployment, operations and maintenance, or use of AI-integrated systems must comply with this IRM and related IRS AI requirements, guidance, and processes, acceptable use agreements, as well as other relevant information disclosure laws, regulations, and policies, including IRC 6103 and the Privacy Act. See IRM 11.3, Disclosure of Official Information, and IRM 10.5.6, Privacy Act.

10.24.1.1.4
(02-10-2026)
Program Management and Review

- (1) Use of AI at the IRS will be managed and reported in accordance with the provisions of this IRM, subject to applicable laws, policies, and security and privacy protections. The CDAO/RAIO oversees all internal and external reporting, including IRS-internal sharing of AI use case inventory details.

10.24.1.1.5
(02-10-2026)
Program Controls

- (1) The CDAO AI team will monitor authoritative sources of federal guidance for new publications or revisions that may affect policies and programs for AI governance at the IRS and will update this IRM and related policies as needed.
- (2) The contents of this IRM provide program controls for all IRS use of AI.

10.24.1.1.6
(02-10-2026)
Terms and Acronyms

- (1) Refer to Exhibit 10.24.1-1, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.24.1.1.7
(02-10-2026)
Related Resources

- (1) Refer to Exhibit 10.24.1-2, Related Resources, for a list of related resources and references.

10.24.1.2
(02-10-2026)
Principles for Use of AI

- (1) As part of IRS AI assurance activities, AI design, development, acquisition, and use must adhere to AI-governing principles established under the Advancing American AI Act and Executive Orders.

- (2) The Advancing American AI Act references these “Principles for Use of AI in Government” outlined in EO 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (Sec. 3):
- a. **Lawful and respectful of the nation’s values**, and consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.
 - b. **Purposeful and performance-driven**, where the benefits of designing, developing, acquiring, and using AI significantly outweigh the risks, and the risks can be assessed and managed.
 - c. **Accurate, reliable, and effective**, where the application of AI is consistent with the use cases for which the AI is trained.
 - d. **Safe, secure, and resilient**, including resilience when confronted with systematic vulnerabilities, adversarial manipulation, and other malicious exploitation.
 - e. **Understandable**, where operations and outcomes of AI must be sufficiently understandable by subject matter experts, users, and others, as appropriate.
 - f. **Responsible and traceable**, such that human roles are clearly defined, AI is used in a manner consistent with its intended purpose, and documentation clearly explains the design, development, acquisition, use, and relevant inputs and outputs of the AI.
 - g. **Regularly monitored and tested** against these principles. Mechanisms should be maintained to supersede, disengage, or deactivate existing applications of AI that demonstrate performance or outcomes that are inconsistent with their intended use or federal requirements.
 - h. **Transparent** in disclosing relevant information regarding the use of AI to appropriate stakeholders, including Congress and the public.
 - i. **Accountable**, where appropriate safeguards for the proper use and functioning of AI must be implemented and enforced, and AI must be appropriately monitored and audited to document compliance with those safeguards.
- (3) From the “Unbiased AI Principles” outlined in EO 14319, Preventing Woke AI in the Federal Government (Sec. 3):
- a. **Truth-seeking**: Large language modes (LLMs) shall be truthful in responding to user prompts seeking factual information or analysis. LLMs shall prioritize historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory.
 - b. **Ideological Neutrality**: LLMs shall be neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as diversity, equity, and inclusion (DEI). Developers shall not intentionally encode partisan or ideological judgments into an LLM’s outputs unless those judgments are prompted by or otherwise readily accessible to the end user.
- (4) OMB may provide additional mandatory and recommended implementation guidance, and the CDAO AI team provides resources to assist project teams in interpreting and applying the AI principles and OMB guidance on the *CDAO AI Governance site*.

10.24.1.3
(02-10-2026)
AI Governance

- (1) The IRS governs AI by use cases- specific scenarios for business use of one or more AI techniques. Effective governance, including AI risk assessment and management, must consider the business context in which AI is being used, and manage risks proportionate to the anticipated risk from its intended use.
- (2) The requirements and recommendations of this IRM apply to system functionality that implements or is reliant on AI, rather than to the entirety of an information system that incorporates AI.
- (3) AI governance processes for reviewing and accepting risk for AI use cases are separate from, do not supersede, and are not all-encompassing of other authorization processes for information systems. IRS business units may establish internal AI use case development and review processes that precede - but do not supersede or replace - service-wide AI governance. Project teams must complete all internal business unit requirements before engaging with enterprise AI use case governance.
- (4) IRS business units and program offices may begin operational use of AI use cases upon receiving approval from an accountable agency official for their business unit or program office. The name of the accountable agency official and the date of their approval must be recorded in the IRS AI Use Case Inventory.
- (5) “Operational use” refers to the deployment or implementation of AI or its output in a manner that impacts IRS business operations. This term excludes preliminary development or usage in exploratory or research-only contexts that do not affect IRS business operations.

10.24.1.3.1
(02-10-2026)
AI Definition

- (1) From the Advancing American AI Act, AI is defined as:
 - a. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
 - b. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
 - c. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
 - d. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
 - e. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.
- (2) OMB M-25-21 provides further technical context to guide interpretation of this definition of AI:
 - a. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including supervised and unsupervised models, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
 - b. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.

- c. For this definition, no system should be considered too simple to qualify as covered AI due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).
- d. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

10.24.1.3.2
(02-10-2026)
AI Use Case

- (1) An AI use case is a specific scenario in which AI is designed, developed, procured, or used to advance the execution of the IRS's mission and delivery of programs and services, to enhance decision-making, or to provide the public with a particular benefit. An AI use case scenario may use one or more AI models and one or more datasets to achieve its objective(s).
- (2) IRS AI use cases are governed by this IRM once they enter the "pre-deployment" stage of development. "Pre-deployment" means the need for the use case has been expressed, its intended purpose and high-level requirements are documented and funds or resources are allocated to begin development and/or acquisition. "Pre-deployment" requires approval from an accountable agency official.
- (3) IRS AI use cases include, but are not limited to:
 - a. Standalone AI capabilities
 - b. AI that is embedded within other systems or applications
 - c. AI developed by the IRS
 - d. AI developed or procured by third parties on behalf of the IRS for the fulfillment of specific IRS missions
 - e. AI procured by the IRS, including commercial-off-the-shelf (COTS) products that include AI functions
 - f. Paid and free services hosted by external service providers and accessed by IRS personnel or automated processes for IRS business use

10.24.1.4
(02-10-2026)
High-Impact AI Use Cases

- (1) The IRS is required to implement minimum risk management practices to manage risks from high-impact AI use cases. Accountable agency officials are responsible for identifying, assessing, mitigating, and accepting risks from AI use, including high-impact AI.

10.24.1.4.1
(02-10-2026)
High-Impact AI Definition

- (1) High-impact AI is defined by OMB M-25-21 as AI whose output serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on:
 - a. an individual or entity's civil rights, civil liberties, or privacy
 - b. an individual or entity's access to education, housing, insurance, credit, employment, and other programs
 - c. an individual or entity's access to critical government resources or services
 - d. human health and safety
 - e. critical infrastructure or public safety
 - f. strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

Ultimately, accountable agency officials must assess each of their AI uses in the context of this definition.

10.24.1.4.2

(02-10-2026)

**Determination of
High-Impact AI**

- (1) Certain uses or expected uses of AI are presumed to be high-impact as defined in OMB M-25-21 and as outlined below. Accountable agency officials must review their AI uses against the uses that are presumed high-impact. The list includes, but is not limited to:
- a. Safety-critical functions of critical infrastructure or government facilities, emergency services, fire and life safety systems within structures, food safety mechanisms, or traffic control systems and other systems controlling physical transit
 - b. Physical movements of robots, robotic appendages, vehicles or craft (whether land, sea, air, or underground), or industrial equipment that have the potential to cause significant injury to humans
 - c. Use of kinetic or non-kinetic measures for attack or active defense in real world circumstances that could cause significant injury to humans
 - d. Transport, safety, design, development, or use of hazardous chemicals or biological agents
 - e. Design, construction, or testing of equipment, systems, or public infrastructure that would pose a significant risk to safety if they failed
 - f. In healthcare contexts, the medically relevant functions of medical devices; patient diagnosis, risk assessment, or treatment; the allocation of care in the context of public insurance; or the control of health-insurance costs and underwriting
 - g. Control of access to, or the security of, government facilities
 - h. Adjudication or enforcement of sanctions, trade restrictions, or other controls on exports, investments, or shipping
 - i. The blocking, removal, hiding, or limitation of the reach of protected speech
 - j. In law enforcement contexts, production of risk assessments about individuals; identification of criminal suspects; forecast of crime; tracking of non-governmental vehicles over time in public spaces; application of biometric identification (e.g., iris, facial, fingerprint, or gait matching); facial reconstruction based on genetic information; social media monitoring; application of digital forensic techniques; use of cyber intrusions; physical location-monitoring or tracking of individuals; detection of weapons or violent activity; or determinations related to recidivism, sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention
 - k. Preparation or adjudication of risk assessments related to foreign nationals seeking temporary or permanent access to the U.S. or its territories including related to immigration, asylum, detention, or travel approval status
 - l. Use of biometric identification for one-to-many identification in publicly accessible spaces
 - m. Ability to apply for, or adjudication of, requests for critical federal services, processes, and benefits to include loans and access to public housing; determination of continued eligibility for ongoing benefits; the control of access-through biometrics or other means (e.g., signature matching)-to IT systems for accessing services for benefits; detection of fraudulent use or attempted use of government services; adjudication of penalties in the context of government benefits
 - n. Determination of the terms or conditions of Federal employment, including preemployment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; reassignment of workers to new tasks or teams

- o. Provision of language translation (e.g., foreign translation and audiovisual translation) when responses are legally binding or for an interaction that directly informs an agency decision or action
 - p. AI that informs or influences whether a taxpayer will be subject to audit, or what aspects of a return will be subject to audit
- (2) Accountable agency officials are empowered to assess whether their AI use case does or does not align to a “presumed high-impact” use.
 - (3) If an accountable agency official assesses that their use case aligns with a presumed high-impact use, they must base any final determination for whether an AI use case is high-impact on the definition of high-impact AI.
 - (4) If an accountable agency official determines that a presumed high-impact use is not, in fact, high-impact, they must document that determination and report it to the CDAO/RAIO through the IRS AI Use Case Inventory.

10.24.1.4.3

(02-10-2026)

**Minimum Risk
Management Practices
for High-Impact AI**

- (1) The IRS takes action and makes decisions that have consequential impacts on the public. If AI is used to perform such action, agencies must deploy trustworthy AI, ensuring that rapid AI innovation is not achieved at the expense of the American people or any violations of their trust.

The IRS must implement minimum risk management practices for high-impact AI that could have significant impacts when deployed, and to prioritize the use of AI that is safe, secure, and resilient. Risk management practices for AI should be proportionate to the anticipated risk from its intended use.

- (2) Per detailed OMB M-25-21 requirements available at the *CDAO AI Governance site*, project teams must implement all of the following minimum risk management practices for high-impact AI use cases:
 - a. Conduct pre-deployment testing
 - b. Complete **AI impact assessment**, see IRM 10.24.1.4.3 (3), Minimum Risk Management Practices, for required elements.
 - c. Conduct ongoing monitoring for performance and potential adverse impacts
 - d. Ensure adequate human training and assessment
 - e. Provide additional human oversight, intervention, and accountability
 - f. Offer consistent remedies or appeals
 - g. Consult and incorporate feedback from end users and the public
- (3) The **AI impact assessment** must contain at least the following elements:
 - a. The intended purpose for the AI and its expected benefit
 - b. The quality and appropriateness of the relevant data and model capability
 - c. The potential impacts of using AI
 - d. Reassessment scheduling and procedures
 - e. Related cost analysis
 - f. Results of independent review
 - g. Risk acceptance

<div>10.24.1.4.4</div> <div>(02-10-2026)</div> <div>Requests for Waivers from High-Impact AI Minimum Risk Management Practices</div>	<div>(1) IRS accountable agency officials may draft a system-specific and context-specific written risk assessment, declaring that fulfilling one or more requirements would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations.</div> <div>(2) The Treasury CAIO, with advisement by the IRS CDAO/RAIO and the DASIB, may waive one or more minimum risk management practices. The authority to approve a waiver is not delegable to any IRS personnel.</div> <div>(3) Annually, the accountable agency official must justify - and the Treasury CAIO must certify - the ongoing necessity of each waiver.</div> <div>(4) The Treasury CAIO may revoke a previously issued waiver at any time.</div>
<div>10.24.1.4.5</div> <div>(02-10-2026)</div> <div>Tracking and Reporting of Determinations, Certifications, and Waivers</div>	<div>(1) To the extent consistent with law and government wide policy, the CDAO/RAIO must centrally track and report each of the following to the Treasury CAIO: <div> <div>a. Accountable Agency Official's determination of high-impact AI.</div> <div>b. DASIB certification for high-impact AI pilot projects to proceed without one or more minimum risk management practices, along with the justification.</div> <div>c. Treasury CAIO waiver of one or more minimum risk management practices for deployed high-impact AI, along with the justification.</div> </div> </div>
<div>10.24.1.4.6</div> <div>(02-10-2026)</div> <div>Termination of Non-Compliant AI</div>	<div>(1) When high-impact AI is not performing at an appropriate level, accountable agency officials must develop and execute a plan to discontinue its use until actions are taken to achieve compliance OMB M-25-21 and this IRM.</div> <div>(2) If proper risk mitigation is not possible, the IRS must cease the use of the AI by suspending access, halting operations, securing data, and initiating remediation.</div>
<div>10.24.1.5</div> <div>(02-10-2026)</div> <div>AI Use Case Inventory</div>	<div>(1) In accordance with the Advancing American AI Act, EO 13960, and OMB M-25-21, the IRS must maintain an inventory of all IRS AI use cases to comply with government-wide reporting requirements.</div> <div>(2) The CDAO/RAIO will oversee the collection, maintenance, and review of the agency's AI use case inventory. The CDAO AI team will review inventory entries to ensure project teams use plain language responses, where appropriate. As part of their efforts to use plain language, project teams should avoid or minimize the use of acronyms and should define any acronyms when first used.</div> <div>(3) The IRS follows guidance from OMB and Treasury regarding the specific information to include in the AI use case inventory and the entries and data fields required for external reporting, including public reporting. Guidance from OMB and Treasury may be updated periodically, and the CDAO AI team will track, implement, and communicate all relevant updates.</div> <div>(4) Certain AI use cases may be exempted from external reporting, in accordance with public law, EO, OMB, or Treasury guidance.</div> <div>(5) External reporting for the annual OMB-directed use case inventory report is coordinated by the CDAO/RAIO through the Treasury CAIO, including public</div>

reporting of determinations, waivers, and related justifications, to the extent consistent with law and government-wide policy.

10.24.1.5.1
(02-10-2026)

**Requirements for the
Inventory of AI Use
Case(s)**

- (1) The IRS AI use case inventory is a comprehensive catalog of AI research and business use scenarios, guided by OMB instructions to agencies for the collection, reporting, and publication of information about agency AI use.
- (2) In general, all IRS **AI use cases in the pre-deployment, pilot, deployed, or retired stage** of development must be entered into the IRS AI Use Case Inventory by the accountable agency official, project lead, or project team.
- (3) When multiple business units are involved with an AI use case, project teams or working groups should designate the person(s) responsible for entering and maintaining the use case inventory entry, and should not duplicate entries for the same use case.

Note: Instructions for accessing the IRS AI Use Case Inventory and creating or updating entries can be found on the *CDAO AI Governance site*. Access permissions are required to view or edit an inventory entry.

- (4) Certain IRS AI use cases that rely principally or exclusively on commercial off-the-shelf (COTS) AI products and services may be eligible for consolidated reporting in the AI use case inventory when all of the following are true:
 - a. The AI is integrated in a COTS product or service.
 - b. The AI use meets one or more of the OMB-provided “widely used AI use cases.”
 - c. The AI use is NOT “high-impact” or substantially customized beyond product’s/service’s default features, capabilities, and interfaces.

The CDAO AI team coordinates the cyclic IRS-wide consolidated AI use case inventory control activity.

- (5) The following are exceptions from requirements to create and maintain AI use case entries and should NOT be recorded in the IRS AI Use Case Inventory:
 - a. AI when it is being used either as a component of any *National Security System* or within the Intelligence Community.
 - b. AI used incidentally by a contractor during performance of a contract (e.g., AI used at the option of a contractor when not directed or required to fulfill IRS requirements).
 - c. IRS assessments of AI applications exclusively because the AI provider is the target or potential target of a regulatory enforcement, law enforcement, or national security action, and not because the IRS is also evaluating such AI applications for IRS use.
- (6) Any IRS business unit with AI use cases that are not excepted from entry and that cannot be recorded in the IRS AI Use Case Inventory for reasons of special sensitivity or national security information classification, must:
 - a. Record those use cases in a database in a manner consistent with OMB and Treasury requirements and this IRM.
 - b. Record all OMB-mandated data fields for those use cases.
 - c. Declare the database to the CDAO/RAIO, including the names of the accountable agency official(s) charged with maintaining the database, and a count of the number of use cases recorded in the database.

- d. Make the database available for oversight and reporting purposes through appropriate channels and with appropriate safeguards, when notified by CDAO/RAIO.

10.24.1.5.2
(02-10-2026)
Inventory Entries

- (1) All IRS accountable agency officials, project leads, and project teams are responsible for documenting their uses of AI in the AI use case inventory, and for following all applicable guidance in this IRM.
- (2) Responsible parties must create and complete required fields for all AI use cases in the “pre-deployment” or later stages in the inventory. This must be done as soon as possible upon approval from the accountable agency official, but no later than the deadline specified by the CDAO/RAIO in advance of the annual OMB-directed use case inventory report.
- (3) AI Use Case Inventory entries must answer all mandatory questions and provide responses with the accuracy, clarity, and detail necessary for a layperson to understand the use case.

Note: IRS business units may establish internal AI use case development and review processes that precede - but do not supersede or replace - service-wide AI governance. Project teams must complete all internal business unit requirements before use cases enter pre-deployment or later stages and are entered into the IRS AI Use Case Inventory.

Note: Avoid including sensitive details in free-text fields whenever it is possible to otherwise describe the use case accurately, clearly, and with sufficient detail.

- (4) When IRS AI use cases leverage COTS or other contract-acquired or contractor-developed AI, the project team must consult with Office of the Chief Procurement Officer (OCPO) and work closely with the vendor or contractor to include certain contractual provisions and collect all relevant information to ensure compliance with OMB M-25-22 and M-26-04 for Large Language Models (LLMs) and answer all OMB-mandatory AI use case inventory questions, including:
 - a. Obtaining documentation from the contractor or vendor that facilitates transparency and explainability, and that ensures an adequate means of understanding what the model does, tracking model performance and effectiveness for procured AI.
 - b. Identifying circumstances that merit including a provision in a solicitation requiring disclosure of AI use as part of any given contract’s performance.
 - c. Disclosing in solicitations whether a planned use of an AI system meets the threshold of a high-impact use case or if there is a reasonable likelihood for such a high-impact use case to occur during the life of the contract.
 - d. For AI systems with potential or expected high-impact use cases, informing vendors and contractors of reasonable transparency and documentation requirements that will be placed on the vendor to enable agency compliance with the requirements in OMB Memorandum M-25-21. For example, project teams should require sufficient descriptive information from vendors to complete the required AI Use Case Inventory entries and AI Impact Assessment for high-impact use cases.

- e. Requiring vendors to provide a notification to the accountable agency official and project team prior to the integration of new AI enhancements, features, or components into systems and services being delivered under contract. Vendor notification to agencies should follow existing processes, where practicable, and should be determined by the relevant agency stakeholders. Project teams should also ensure, prior to contract release, that compliance requirements will be followed, consistent with OMB Memorandum M-25-21.
 - f. For each Federal contract for an LLM requiring that the procured LLM comply with the EO 14319-defined Unbiased AI Principles and providing that decommissioning costs shall be charged to the vendor in the event of termination by the IRS for the vendor's noncompliance with the contract following a reasonable period to cure.
 - g. To the extent practicable and consistent with contract terms, revising existing contracts for LLMs to include the terms specified in Sec. 4.(b)(i) of EO 14319.
 - h. Adopting procedures to ensure that LLMs procured by the IRS comply with the EO 14319-defined Unbiased AI Principles.
- (5) Where a sensitive use case name or details must be included to understand the use case, project teams must mark the overall use case to be "withheld" from public reporting, and clearly portion-mark the sensitive portions with sensitive but unclassified (SBU), PII, federal taxpayer information FTI, or other relevant marking in accordance with IRM 10.5.1.6.5, Marking.
- (6) Failure by the AI project team to properly flag the use case name and/or details as sensitive (required to be withheld from public reporting) may lead to unintended public or other disclosure.

Note: As the IRS AI Use Case Inventory is an unclassified repository on an unclassified network, entries must not contain any classified AI use case names or other descriptive information (e.g., confidential, secret, top secret, or sensitive compartmented information).

10.24.1.5.3
(02-10-2026)
**Inventory Maintenance
and Validation**

- (1) AI project teams must maintain the accuracy and currency of their information in the use case inventory. Project teams must update the inventory record when a change occurs to the use case that meaningfully affects the accuracy of the current record, including but not limited to changes in stage of development, high-impact AI determination, purpose and expected benefits, etc.
- (2) Project teams must review and validate their inventory record(s) at least annually.
- (3) Project teams must validate or update their inventory record(s) when otherwise directed by the CDAO AI team.

Note: IRM 10.8.1.4.13.5, PM-05 System Inventory, contains guidance regarding the IRS AI Use Case Inventory that is superseded by the guidance in this IRM if the two are in conflict (paragraph 12).

10.24.1.6
(02-10-2026)
**AI Model and Data
Inventory**

- (1) In accordance with Executive Order 13859, Maintaining American Leadership in Artificial Intelligence, Section 5(a), the IRS requires model and data inventory entries for each model, algorithm, method, and dataset affiliated with an AI use case. These entries must be completed by AI project teams when the use case enters the "deployed" stage of development.

- (2) Project teams are required to update model and data inventory entries when there are changes that significantly impact the accuracy of the current entries. Additionally, these entries must be reviewed and validated by the project team at least annually, or when directed by the CDAO AI team.
- (3) Examples of changes that require updates may include:
 - a. Changing the context, scope, or intended purpose of the use case.
 - b. Changing the use case's output or impact on IRS operations.
 - c. Updating or retraining the underlying AI model(s).
 - d. Incorporating new data elements or data sources.
- (4) Job aids for the model and data inventory entries can be found on the *CDAO AI Governance* site.

10.24.1.7

(02-10-2026)

Generative AI (GenAI)

Policy

- (1) This policy sets the terms for acceptable use of generative AI for the IRS mission and establishes safeguards and oversight mechanisms that allow generative AI to be used without posing undue risk. IRS use of generative AI must also conform to the Treasury Artificial Intelligence System User Agreement hosted on the *my.treasury.gov Artificial Intelligence and Large Language Models* site.

10.24.1.7.1

(02-10-2026)

Generative AI (GenAI)

Definition

- (1) Generative AI is defined as the class of AI models that generate AI-derived output such as images, videos, audio, text, and other digital content.

10.24.1.7.2

(02-10-2026)

Prohibited Uses of

GenAI

- (1) IRS GenAI users must always ensure the use of only Treasury- or IRS-approved GenAI products and services and strictly comply with the guidelines established in this policy and in alignment with guidance from the Treasury Chief Information Officer (CIO), Treasury CAIO, IRS CDAO/RAIO, or other IRS authority. IRS GenAI users assume responsibility for ensuring the accuracy and legality of the data they upload or input into the AI systems, and the data that is output from them before it may be shared.
- (2) IRS GenAI users are bound by the Treasury AI User Agreement, including but not limited to prohibition of the following:
 - a. Use of any AI system that has not been approved for execution of the Treasury mission. Users seeking the use of AI systems provided by other government agencies should enter into a Memorandum of Understanding or similar agreement.
 - b. Input or upload into any public, non-Treasury, or otherwise-unauthorized AI system: personally-identifiable information (PII), federal taxpayer information (FTI), acquisition sensitive information, Bank Secrecy Act (BSA) information, statutorily-protected tax information, export-controlled or critical infrastructure controlled unclassified information (CUI), classified information, Official Use Only (OUO) information, Agency proprietary business information (PBI), other Sensitive But Unclassified (SBU) information, or any other non-public record or information that the Department has identified as restricted in nature and/or that the release of which could cause harm to the United States Government, the Treasury, or the IRS.
 - c. Use AI systems for any unethical or illegal purpose.

- d. Input or upload data that is defamatory or infringing on any intellectual property rights.
- e. Tampering or security evasion including attempts to reverse engineer, decompile, or disassemble any part of the AI systems except where required to meet Treasury mission requirements.
- f. Engage in any activity that disrupts or interferes with the integrity or performance of the AI systems.
- g. Use any outputs from AI systems in the performance of government business without ensuring direct human review to confirm the veracity of the information.
- h. Using AI-generated content without reviewing the accuracy and appropriateness of the information.
- i. Obfuscation of AI origin - when using GenAI to generate content, you must be transparent about AI use. As appropriate, disclose that the content was created with the assistance of and how GenAI was used (e.g. drafting, editing, etc.).

Undertaking any of the above prohibited uses may be the basis of disciplinary action, up to and including removal from federal service.

10.24.1.7.3
(02-10-2026)
GenAI Guidelines

- (1) Employees must be aware that entering any information, including seemingly innocuous work-related matters, into public or non-Treasury AI tools (such as publicly accessible chatbots or AI writing assistants) can pose significant risks. Publicly-available platforms and services typically retain, reuse, or resell entered information, potentially resulting in unintended disclosure of IRS internal strategies, plans, or intentions. Information that appears non-sensitive at first glance could compromise IRS operational planning, decision-making, confidentiality, or security when aggregated or analyzed externally.
 - a. IRS uses of GenAI must be approved by an accountable agency official and align with IRS mission objectives and comply with applicable legal, privacy, and civil liberties requirements.
 - b. IRS GenAI systems must be governed by user agreements; employees must review, accept, and follow all requirements established in such agreements.
 - c. Employees are responsible for their inputs as prompts to solicit AI-generated outputs, and for their use, publication, or distribution of those outputs for internal or external purposes. Employees must review GenAI outputs to ensure they are appropriate for further use.
 - d. Users must maintain strong safeguards for civil rights, civil liberties, and privacy in their use of GenAI while also promoting innovation and public trust.
 - e. GenAI use cases must be reviewed against the list of uses that are “presumed” high-impact AI (see IRM 10.24.1.4.2 , Determination of High-Impact AI). GenAI use cases with outputs that serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on rights or safety must be determined as ‘high-impact’ and subject to enhanced risk management and oversight consistent with M-25-21, Section 4. Refer to IRM 10.24.1.4, High-Impact AI Use Cases.
 - f. IRS must ensure that any generative AI systems procured or deployed for federal purposes demonstrate ideological neutrality, prioritizing truthfulness and historical accuracy, and explicitly avoid embedding or promoting ideological constructs associated with diversity, equity, and inclusion (DEI) or similar social agendas (Per EO Preventing Woke AI in the Federal Government).

- g. The use of GenAI tools to create deceptive, misleading, or other content that violates law or policy is expressly prohibited. Do not use GenAI to make binding determinations or actions on taxpayer rights without proper oversight (see IRM 10.24.1.4, High-impact AI Use Cases), generate taxpayer-facing communications without appropriate validation, process or synthesize information in ways that risk disclosure of taxpayer data, including OUO, PII or FTI, unless explicitly authorized and protected.
- h. IRS-controlled GenAI must include a user agreement and a problem/incident reporting mechanism.

10.24.1.7.4

(02-10-2026)

GenAI Considerations

- (1) Employees should keep the following considerations and best practices in mind as they interact and experiment with LLMs:
 - a. **Accuracy and Reliability:** LLMs may sometimes produce inaccurate or misleading information. LLMs can also produce what are called “hallucinations.” Hallucinations result when output appears coherent and plausible, but does not reflect factual data. Always critically evaluate LLM outputs and verify information from reliable sources.
 - b. **Transparency and Disclosure:** When using LLMs to generate content, be transparent about their involvement. As appropriate, disclose that the content was created with the assistance of an LLM and how AI was used (e.g. drafting, editing, etc.).
 - c. **Variability in Responses:** LLMs may generate different responses to the same prompt if asked more than once. This variability is a normal part of their function, as their output is based upon the probability of the next token as output. Experiment with different prompts and parameters to achieve desired results.
 - d. **Over-reliance:** Avoid becoming overly reliant on LLMs. Use LLMs as tools to assist and augment your work, not replace your own critical thinking and judgment.
 - e. **Consult PGLD at *Privacy** for guidance on requirements for use of data in GenAI contexts, including publicly-available, synthetic, simulated, or anonymized data.

10.24.1.8

(02-10-2026)

AI Recordkeeping Requirements

- (1) AI use case records must be retained per IRS record control schedules unless such requirements are waived for a specific AI use case or IT system under other statutory or regulatory provisions:
 - a. AI use case documentation: Life + 3 years (per OMB M-25-21 & NARA GRS 3.1)
 - b. AI prompt logs: 1 year (per NARA GRS 5.2)
 - c. AI test logs: Until replaced
 - d. AI system incident logs: Life (Per IRM 10.8)

10.24.1.9

(02-10-2026)

Protection of Taxpayer Rights

- (1) The Internal Revenue Code (IRC) lists specific taxpayer rights which are further explained in The Taxpayer Bill of Rights. See IRC 7803(a)(3); Publication 1, Your Rights as a Taxpayer; and the *Taxpayer Bill of Rights*.
- (2) IRS employees are responsible for being familiar with and acting in accordance with these rights. IRS use of AI must not violate these rights.

10.24.1.10
(02-10-2026)

**Privacy and Security
Requirements**

- (1) AI use cases must follow all relevant IRS privacy and security policies, such as those set forth in IRM 10.5, Privacy and Information Protection, and IRM 10.8, Information Technology (IT) Security.
- (2) AI systems must include audit trails for all access to and processing of SBU/ CUI including PII and FTI. Users must acknowledge responsibility for handling of sensitive data in accordance with system user agreements and any applicable business unit requirements.
- (3) In particular, those developing, procuring, or using AI must follow requirements in these IRM subsections where applicable:
 - IRM 10.5.1.6, Practical Privacy Policy
 - IRM 10.5.2.2, Privacy and Civil Liberties Impact Assessment (PCLIA)
Note: NOTE: For an explanation of civil liberties, see IRM 10.5.2.2.2.1, Civil Liberties
 - IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs)
 - IRM 10.5.6.5, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections)

Exhibit 10.24.1-1 (02-10-2026)
Terms and Acronyms

The following table contains terms and acronyms used throughout this IRM.

Term	Definition
Artificial Intelligence (AI)	<p>In accordance with the Advancing American AI Act, the term “artificial intelligence” or “AI” has the meaning provided in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019:</p> <ol style="list-style-type: none"> Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. A set of techniques, including machine learning, that is designed to approximate a cognitive task. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting. <p>OMB M-25-21 provides additional technical context to guide interpretation of this definition of AI:</p> <ol style="list-style-type: none"> This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including deep learning as well as supervised, unsupervised, and semisupervised approaches), reinforcement learning, transfer learning, and generative AI. For this definition, no system should be considered too simple to qualify as covered AI due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes). This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

Exhibit 10.24.1-1 (Cont. 1) (02-10-2026)**Terms and Acronyms**

Term	Definition
AI Assurance Team (AIAT)	The AIAT is a cross-functional team of leaders and subject matter experts (SMEs) from several business units, including PGLD, Counsel, IT/Security, RAAS & others. The AIAT serves as “independent reviewer” to ensure that necessary “high-impact AI” minimum risk management practices are completed and meet IRS policy requirements. The AIAT also advises the CDAO/RAIO via the DASIB on whether to reconsider an accountable agency official’s determination that a particular AI use case – though presumed to be high-impact – is not actually high-impact.
AI Dataset	An AI dataset is a structured collection of data, often used for analysis and decision-making, accessible to or through, integrated into, or generated by the AI elements of the use case.
AI Model	An AI model means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.
AI Use Case	An AI use case is a specific scenario in which AI is designed, developed, procured, or used to advance the execution of the IRS’s mission and delivery of programs and services, to enhance decision-making, or to provide the public with a particular benefit. An AI use case scenario may use one or more AI models and one or more datasets to achieve its objective(s).
Accountable Agency Officials	IRS leaders generally in executive or managerial roles - or their properly designated acting equivalents - who are trained and empowered to identify, assess, mitigate, and accept risk for one or more AI use cases, and who are accountable for the mission outcome of the AI use case(s). IRS business unit leaders may determine who is truly “accountable” for the mission outcome of the AI use case.
CAIO	Chief AI Officer. The CAIO is a Treasury-level role with authority to delegate most, but not all, OMB-specified AI governance authorities and responsibilities.
CDAO	Chief Data and Analytics Officer. Refer to IRM 1.1.18.1, Research, Applied Analytics and Statistics Division, for a detailed description of responsibilities.
DASIB	Data & Analytics Strategic Integration Board. DASIB’s mission is to promote and enhance the application of data and analytics solutions to improve IRS operations and mission effectiveness. The DASIB will integrate relevant organizational perspectives to set strategic priorities, facilitate knowledge sharing and enhance leadership visibility into data and analytics (D&A) products and activities, direct and approve standards to enhance the accessibility and usability of data and analytics Service-wide, and serve as the IRS Artificial Intelligence Governance Board for certain matters pertaining to high-impact AI.

Exhibit 10.24.1-1 (Cont. 2) (02-10-2026)
Terms and Acronyms

Term	Definition
Determination	A determination is the result of IRS accountable agency official and AI project team evaluation of the AI use case’s specific output(s) and potential risks when assessing and determining the applicability of the high-impact definition. An accountable agency official must submit written documentation to notify the CDAO/RAIO when making a determination that a particular AI use case that is presumed to be high-impact per OMB M-25-21 Sec. 6 does not actually meet the definition of high-impact AI.
EO	Executive Order
GenAI	The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.
High-Impact AI	<p>High-impact AI is AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on:</p> <ol style="list-style-type: none"> 1. An individual or entity’s civil rights, civil liberties, or privacy; or 2. An individual or entity’s access to education, housing, insurance, credit, employment, and other programs; 3. An individual or entity’s access to critical government resources or services; 4. Human health and safety; 5. Critical infrastructure or public safety; or 6. Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government. <p>Certain uses of AI are presumed to be high-impact (see IRM 10.24.1.4, High-Impact AI Use Cases). AI may be integrated in decision or activity pipelines in high-impact categories without meeting the definition of high-impact when the AI’s output does not actually “serve as a principal basis for” the relevant type of agency action or decision.</p>
IRC	Internal Revenue Code
IT	Information Technology
Minimum Risk Management Practices for High-Impact AI	OMB M-25-21 Sections 4.b.i-vii (pages 15-17) describe the comprehensive set of minimum requirements that agencies must implement for high-impact AI use cases. Exemption from any one or more minimum requirements requires an approved waiver from the Treasury CAIO.
OMB	Office of Management and Budget
Operational Use	“Operational use” means AI or its output is in the “pilot” or “deployed” stage of development and put into service in a way that affects IRS business operations. It does not include preliminary development or use in exploratory or research-and-development-only contexts that do not affect IRS business operations.
PCLIA	Privacy and Civil Liberties Impact Assessment
RAAS	Research, Applied Analytics and Statistics

Exhibit 10.24.1-1 (Cont. 3) (02-10-2026)**Terms and Acronyms**

Term	Definition
RAIO	Responsible Artificial Intelligence Official
Waiver	A waiver is a formal exemption from one or more of the required minimum risk management practices for high-impact AI, granted by the Treasury CAIO after a documented, system-specific risk assessment. All waivers must be written, justified, centrally tracked, and annually re-certified, and may be revoked at any time. The Treasury CAIO's authority to grant waivers may not be delegated.

Exhibit 10.24.1-2 (02-10-2026)

Related Resources

Public Laws

- Advancing American AI Act

Executive Orders

- *Executive Order 13859*, Maintaining American Leadership in Artificial Intelligence
- *Executive Order 13960*, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government
- *Executive Order 14179*, Removing Barriers to American Leadership in Artificial Intelligence

Office of Management and Budget Memoranda

- OMB M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust
- OMB M-25-22, Driving Efficient Acquisition of Artificial Intelligence in Government
- OMB Fact Sheet: Driving Efficient Acquisition of Artificial Intelligence in Government
- OMB 2025, Guidance for AI Use Case Inventories
- OMB 2025, Questions for AI Use Case Inventories

IRS Publications

- IRM 10.5.1, Privacy Policy
- IRM 10.5.2, Privacy Compliance and Assurance (PCA) Program
- IRM 10.5.6, Privacy Act
- IRM 10.8.1, Security Policy
- IRM 10.8.2, IT Security Roles and Responsibilities
- Publication 1, Your Rights as a Taxpayer

