RESEARCH, APPLIED ANALYTICS
AND STATISTICS

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 20, 2024

Control Number: RAAS-10-0524-0001
Expiration Date: May 19, 2026
Affected IRM: NEW 10.24.1

MEMORANDUM FOR ALL SENIOR EXECUTIVES

FROM: Barry Johnson
Chief Data and Analytics Officer (CDAO) and Responsible AI Official (RAIO)

Barry W. Johnson
Digitally signed by Barry W. Johnson
Date: 2024.05.21 13:53:06 -04'00'

SUBJECT: Interim Guidance for New IRM 10.24.1, *Artificial Intelligence (AI) Governance and Principles*

This interim guidance memorandum is issued to communicate Artificial Intelligence (AI) governance and principles. The content is being released as interim guidance to facilitate timely implementation of the AI guidance.

This guidance establishes policies relating to governance of AI at the IRS. It specifies the AI governance process, including the IRS AI use case inventory and steps necessary for AI use cases to receive approval to operate in a production workflow. It also codifies IRS responsibilities relating to OMB M-24-10, *Advancing Governance, Innovation, and Risk Management of Agency Use of Artificial Intelligence*, such as minimum practices required to use safety-impacting or rights-impacting AI.

Please distribute the attached new IRM 10.24.1, *Artificial Intelligence (AI) Governance and Principles* to all personnel responsible for developing, procuring, using, and monitoring AI. This policy applies to all employees, contractors, and vendors of the IRS.

Purpose: IRM 10.24.1, *Artificial Intelligence (AI) Governance and Principles*, is being published as interim guidance until the IRM becomes available via the normal publishing process.

Effect on Other Documents: This is new guidance.

Effective Date: May 20, 2024

Contact: Please send questions or inquiries related to this guidance to [redacted].

Attachment: Proposed New IRM 10.24.1, *Artificial Intelligence (AI) Governance and Principles*

cc: FOIA Library on IRS.gov

Manual Transmittal **Month DD, YYYY**

Purpose

(1) This transmits new Internal Revenue Manual (IRM) 10.24.1, Artificial Intelligence, Artificial Intelligence (AI) Governance and Principles.

Material Changes

(1) This new IRM establishes requirements and recommendations for internal and external Internal Revenue Service (IRS) development, implementation, and use of AI.

Effect on Other Documents

This is a new IRM.

Audience

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

Effective Date

(MM-DD-YYYY)

Signature

Barry W. Johnson
Chief Data and Analytics Officer

IRM

Part 10
Security, Privacy, Assurance and Artificial Intelligence

Chapter 24
Artificial Intelligence
Section 1
Artificial Intelligence (AI) Governance and Principles

Table of Contents

List of Exhibits

10.24.1.1 (MM-DD-YYYY)
Program Scope and Objectives

(1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage the use of artificial intelligence (AI) within the Internal Revenue Service (IRS).

(2) **Purpose of the Program:** Develop and publish governance policies to create trust in the use of AI through responsible AI practices, and ensure compliance with federal mandates and legislation. Harness the benefits of AI while mitigating its risks.

(3) **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.

(4) **Policy Owner:** Chief Data and Analytics Officer (CDAO), who also serves as the Responsible AI Official (RAIO).

(5) **Program Owner:** The office of the CDAO, whose executive serves as the RAIO, is the program office responsible for overseeing the IRS AI governance program.

(6) **Program Goals:** To ensure the responsible use of AI at the IRS.

10.24.1.1.1 (MM-DD-YYYY)
Background

(1) Between 2019 and 2023, legislation and federal guidance drove the need to ensure trustworthy use of advanced analytics and artificial intelligence. Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, called for the development and implementation of nine trustworthy AI guiding principles by agencies and the collection of an annual AI use case inventory. Legislation such as the National Artificial Intelligence Initiative (NAAI) in 2020 and AI in Government Act of 2020 was signed. In October 2022, the White House Office of Science and Technology Policy released the "*Blueprint for an AI Bill of Rights*," which identified five principles to guide the design, use, and deployment of automated systems to protect the American public in the age of AI. The National AI Initiative Office, the National Institute for Standards and Technology *AI Risk Management Framework (NIST AI RMF)*, and the General Services Administration (GSA) AI Center of Excellence provide additional guidance, direction, and coordination on AI practices.

(2) In 2022, an IRS Advanced Analytics and Artificial Intelligence Strategy (AI Strategy) was adopted by the Data and Analytics Strategic Integration Board (DASIB). The Strategy was driven by requirements from Executive Order 13960. The AI Strategy is intended to help the IRS address its current and future challenges. The IRS' existing Data & Analytics Operating Model entities (see *IRM 1.7.1.2*, IRS Research Program Management, Oversight and Coordination) will continue to be used to govern the execution of the AI Strategy. As the IRS' Responsible AI Official (RAIO), the IRS' Chief Data and Analytics Officer (CDAO) will oversee AI governance and take a lead role in reviewing and validating advanced analytics to ensure their trustworthy use.

(3) In 2023, Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023) instituted the new agency role of Chief

Artificial Intelligence Officer (CAIO), and in response the Department of Treasury has designated a department-level CAIO. Executive Order 14110 also requires agencies to develop guidelines, standards, and best practices for AI reliability, safety, and security—with particular focus on AI uses that impact rights and safety—and specifies safeguards relating to privacy and protected populations. In parallel, OMB Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (March 28, 2024) defines CAIO roles and responsibilities and formalizes agency actions related to AI governance (e.g., AI use case inventories, coordination around use of AI, risk management, and more). OMB M-24-10 also puts forward specific requirements, such as minimum risk-management practices for safety-impacting or rights-impacting AI.

(4) With the passing of the Inflation Reduction Act (IRA) and the subsequent development of the *IRA Strategic Operating Plan (IRA SOP)*, the IRS further recognizes data and analytics governance is a critical enabler for all data-related initiatives and data-driven decision-making. The IRA SOP specifically calls for enhanced, enterprise-wide data governance to facilitate effective application of data to mission goals. Furthermore, many of the IRA SOP initiatives are dependent on effective, collaborative data governance.

(5) Effective governance promotes collaborative dialogue across disparate business units, empowers employees by enhancing data literacy and raising awareness of data resources, facilitates standardization, fosters data linkages, creates clear lines of authority to ensure data quality, and provides a clear path of escalation for data-related problems. These are all needed attributes to realize many of the data-dependent IRA initiatives.

10.24.1.1.2 (MM-DD-YYYY)
Authority

(1) The CDAO authorization to oversee enterprise-level data and analytics activity is designated in the *Evidence-Based Policymaking Act* and the *Taxpayer First Act Report to Congress*.

(2) All IRS information systems and technologies must be compliant with directives and guidance from executive orders (EOs), the Office of Management and Budget (OMB), the Federal Information Security Modernization Act of 2014 (FISMA), the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), the National Archives and Records Administration (NARA), the Department of the Treasury, and the IRS, as they apply.

(3) *AI in Government Act of 2020*. See Pub. L. No. 116-260, div. U, title 1, 104 (codified at 40 USC 11301 note).

(4) *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).

(5) *National Institute for Standards and Technology AI Risk Management Framework (NIST AI RMF)*.

(6) *Blueprint for an AI Bill of Rights*.

(7) Presidential *EO 13960*, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government.

(8) Presidential *EO 14110*, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

(9) *OMB Memorandum M-24-10*, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.

10.24.1.1.3 (MM-DD-YYYY)
Roles and Responsibilities

(1) The Chief Data and Analytics Officer (CDAO) acts as the Responsible AI Official (RAIO) to oversee IRS implementation of OMB M-24-10 requirements and support the Treasury CAIO in fulfilling department-level M-24-10 responsibilities as they relate to the IRS. The CDAO, as RAIO, is responsible for coordination of AI within the IRS. See *IRM 10.24.1.3*, Responsible Artificial Intelligence Official (RAIO).

(2) Senior executives in each business unit are responsible for conducting and managing AI use within their business units in compliance with this IRM and other applicable policies. They are also responsible for coordinating all AI activity through the AI Governance Project Management Office (PMO).

(3) Executives in each business unit are responsible for following the policies in *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).

(4) The Data and Analytics Strategic Integration Board (DASIB) is the ultimate decision-making body for approval to use artificial intelligence within the IRS. See *IRM 1.7.1.2.1*, Data and Analytics Strategic Integration Board Purpose and Scope, for information on DASIB membership and additional roles, and *IRM 10.24.1.5.1*, AI Governance Key Stakeholders and Responsibilities, for additional information on DASIB's roles and responsibilities in the governance process.

(5) The AI Governance Project Management Office (PMO) is a team of IRS employees and/or contractors who facilitate and administrate the AI governance process. See *IRM 10.24.1.5.1*, AI Governance Key Stakeholders and Responsibilities, for additional responsibilities of the AI Governance PMO.

(6) Employees are responsible for complying with this IRM and related IRS AI requirements and guidance.

10.24.1.1.4 (MM-DD-YYYY)
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, as RAIO, will oversee all internal and external reporting.

10.24.1.1.5 (MM-DD-YYYY)
Program Controls

(1) The Office of the CDAO will continuously monitor federal guidance for revisions that may affect policies and programs for AI governance at the IRS and will update this IRM and related policies as needed. Program controls include the AI use case inventory, AI governance process, and other control mechanisms contained in this IRM section.

10.24.1.1.6 (MM-DD-YYYY)
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 (MM-DD-YYYY)
Related Resources

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

10.24.1.2 (MM-DD-YYYY)
Principles for Use of AI in Government

(1) According to the principles set forth in Executive Order 13960, IRS design, development, acquisition, and use of AI must be:

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.

10.24.1.3 (MM-DD-YYYY)
Responsible Artificial Intelligence Official (RAIO)

(1) In accordance with EO 14110 and OMB M-24-10 Section 3(b)(ii), the Department of Treasury Chief AI Officer (CAIO), in coordination with other responsible officials, bears primary responsibility for Department of Treasury compliance with the requirements of OMB M-24-10. At the IRS, the Chief Data and Analytics Officer (CDAO) acts as the Responsible AI Official (RAIO) to oversee bureau-level implementation of OMB M-24-10 requirements and support the Treasury CAIO in fulfilling the following responsibilities as they relate to the IRS:

a) Maintaining awareness of AI activities, including through creating and maintaining the AI use case inventory. (OMB M-24-10 Section 3(b)(ii)(C))
b) Identifying and removing barriers to the responsible use of AI, including through the advancement of AI-enabling enterprise infrastructure, workforce development measures, policy, and other resources for AI innovation, without violating laws. (OMB M-24-10 Section 3(b)(ii)(L)).
c) Managing a program that supports the identification and management of risks from the use of AI, especially for safety-impacting or rights-impacting AI. (OMB M-24-10 Section 3(b)(ii)(O))
d) Working with relevant senior officials to establish or update processes to measure, monitor, and evaluate the ongoing performance of AI applications and whether they are achieving their intended objectives. (OMB M-24-10 Section 3(b)(ii)(P))
e) Overseeing compliance with requirements to manage risks from the use of AI, including those established in OMB M-24-10 and in relevant law and policy such as the NIST AI Risk Management Framework. (OMB M-24-10 Section 3(b)(ii)(Q))
f) Conducting risk assessments, as necessary, of AI applications to ensure compliance with OMB M-24-10. (OMB M-24-10 Section 3(b)(ii)(R))
g) Waiving individual applications of AI from elements of OMB M-24-10 Section 5 through the process detailed in that section. (OMB M-24-10 Section 3(b)(ii)(T))
h) Ensuring that the agency does not use AI that is not in compliance with OMB M-24-10, in partnership with relevant agency officials (e.g., authorizing, procurement,

legal, human capital, and oversight officials). This may include assisting these relevant agency officials in evaluating authorizations to operate based on risks from the use of AI. (OMB M-24-10 Section 3(b)(ii)(U))

10.24.1.4 (MM-DD-YYYY)
AI Use Case Inventory

(1) The IRS must maintain an inventory of all its AI use cases and submit inventory updates at least annually to Treasury. Updates may be submitted more frequently if required by Treasury policy. The IRS CDAO, as RAIO, is responsible for the creation and maintenance of the AI use case inventory and oversees associated data collection and submission to Treasury. Treasury is responsible for sharing its department-wide AI use case inventory with other agencies and the public, in accordance with OMB M-24-10 Section 3(a)(iv). Specific use cases may be excluded from external reporting, in accordance with Treasury and OMB guidance; however, no use case is excluded from entry in the internal IRS AI use case inventory.

(2) All IRS business units and program offices are responsible for documenting their uses of AI in the AI use case inventory and following all applicable guidance in this IRM.

(3) All IRS AI use cases must be recorded in the AI use case inventory site upon receiving approval to begin work from program or function leadership (e.g., after a project kick-off meeting is held). AI project teams are responsible for maintaining the accuracy and currency of their use case's information in the AI use case inventory.

Note: #[redacted]#

(4) Each entry in the AI use case inventory of a use case that is safety-impacting or rights-impacting must provide accessible documentation of the system's functionality in plain language. To the extent consistent with applicable law and government-wide guidance, these entries will serve as public notice of the AI to its users and the general public. (OMB M-24-10 Section 5(c)(iv)(I)) See *IRM 10.24.1.8.8*, Public Notice and Plain Language Documentation.

(5) Guidance regarding what specific information must be contained in the AI use case inventory and in what format the inventory must be published is set by Treasury or OMB and may be updated on an annual basis. The IRS will follow all guidance received from Treasury or OMB when maintaining its use case inventory or sharing its inventory with Treasury, other agencies, or the public.

Note: *IRM 10.8.1.4.13.5(12)*, PM-05 System Inventory, contains guidance regarding the IRS AI use case inventory that will be superseded by the guidance in this IRM if the two are in conflict.

10.24.1.5 (MM-DD-YYYY)

AI Governance

(1) This subsection describes the key stakeholders in the IRS AI governance process along with their roles and responsibilities. It also describes governance artifacts and additional requirements.

(2) AI governance will take place at the level of an AI use case, meaning a specific business use of an AI technique. Effective governance, including risk assessment and mitigation, must consider the context in which AI is being used.

10.24.1.5.1 (MM-DD-YYYY)
AI Governance Key Stakeholders and Responsibilities

(1) The **Data and Analytics Strategic Integration Board (DASIB)** is the ultimate decision-making body for approval to use artificial intelligence within the IRS. DASIB will fulfill the following roles:

a) Oversee the portfolio of AI projects at the IRS and ensure compliance with federal requirements.
b) Provide final approval for safety-impacting or rights-impacting AI that will be used in a production workflow. Authorizing Officials for systems containing an AI component must receive DASIB approval of AI capabilities before granting Authorization to Operate.

Note: See *IRM 1.7.1.2.1,* Data and Analytics Strategic Integration Board Purpose and Scope, for information on DASIB membership and additional roles, and *IRM 10.24.1.5.3*, AI Governances Process for AI Use Cases, for information on DASIB's role in the governance process.

(2) The **AI Governance Project Management Office (PMO)** is a team of IRS employees and/or contractors who facilitate and administrate the AI governance process. Their primary roles and responsibilities are as follows:

a) Support project teams in successfully navigating the governance process.
b) Facilitate communication between project teams, DASIB, and the AI Assurance Team (see (3) below).
c) Document compliance with all applicable governance requirements.

(3) The **AI Assurance Team** is a cross-functional team of subject matter experts from PGLD, Counsel, IT, RAAS, TAS, or other Business Operating Divisions (BODs) who will validate AI use case compliance with applicable IRS policies and processes. Their primary roles and responsibilities are as follows:

a) Review a use case's submitted artifacts, including applicable independent assessments, to ensure that necessary assessments are completed in a manner which meets IRS policy requirements. Submitted artifacts and assessments may

include a Privacy and Civil Liberties Impact Assessment (PCLIA), System Security Assessment, Risk of Bias Assessment, and other assessments as applicable.

b) Provide the AI Governance PMO and DASIB an assessment and recommendation of a use case's readiness to be deployed in a production workflow.

(4) **AI Project Teams** are teams of IRS employees and/or contractors in any unit of the IRS working to develop or maintain an AI use case. Teams may include project managers, developers, subject matter experts in the business context, and others. Their primary roles and responsibilities in relation to AI governance are as follows:

a) Work with the AI Governance PMO to prepare governance artifacts and all required reporting inputs for their AI use case(s).

b) Comply with applicable BOD, domain, and enterprise governance requirements, including the One Software Development Lifecycle (OneSDLC) process and any necessary reviews of their use case materials, methodology, or performance metrics.

(5) **Any IRS Business Unit or Office** may contact the AI Governance PMO at their mailbox # [redacted] # for guidance on AI usage and information regarding AI requirements and approval processes. All development, procurement, and implementation of AI must be reported to the AI Governance PMO to ensure compliance with AI requirements. IRS business units or offices may also seek support or guidance form the AI Governance PMO for training, communication, and other actions related to the use of AI.

10.24.1.5.2 (MM-DD-YYYY)
AI Governance Artifacts

(1) This subsection provides a brief description of each AI use case artifact mentioned in *IRM 10.24.1.5.3*, AI Governance Process for AI Use Cases.

a) **Model Card:** Provides detailed documentation explaining the AI model(s) of a particular AI use case, such as expected inputs and outputs, performance metrics, risks of use, limitations, intended user audience, and points of contact.

Note: # [redacted] #

b) **Datasheet:** Provides detailed documentation explaining the data used by a particular AI use case, such as its source, size, provenance, sensitivity, intended use, cleaning/transformation pipelines, and known quality issues.

Note: # [redacted] #

c) **Intake Questionnaire:** A single-point-of-entry mechanism to enter an AI use case into the IRS AI use case inventory and answer questions to facilitate governance review.

Note: #[redacted]#

d) **Risk of Bias Assessment:** An assessment performed to evaluate an AI use case's risk of operating in a biased manner, particularly regarding protected groups or classes.
e) **Readiness Assessment Report:** A report issued by the AI Assurance Team that certifies a use case's compliance with applicable IRS policies regarding privacy, security, etc. and gives a recommendation regarding the use case's readiness to be used in a production workflow.
f) **Project Summary Report:** A report issued by the AI Governance PMO to DASIB that summarizes an AI use case's purpose, benefits, risks, compliance with applicable governance requirements, and recommended monitoring and review plan.

10.24.1.5.3 (MM-DD-YYYY)
AI Governance Process for AI Use Cases

(1) When development of an AI use case is initiated, the project team must complete the Initiation Phase questions of the AI use case Intake Questionnaire to record the use case in the IRS AI use case inventory. See *IRM 10.24.1.5.2*, AI Governance Artifacts.

(2) When an AI use case has been developed and is ready to be used in a production workflow, the process below must be followed. DASIB approval is required for all safety-impacting or rights-impacting AI use cases prior to use in a production workflow.

a) The AI project team must complete the entire IRS AI use case Intake Questionnaire, which includes questions required by the Treasury AI Governance Board for their AI Risk/ Impact Assessment.
b) The AI project team must complete model card and datasheet artifacts. See *IRM 10.24.1.5.2*, AI Governance Artifacts.
c) In coordination with the AI Governance PMO, the AI project team will determine all IRS approval requirements that apply to their use case, according to its risk profile. Requirements may include privacy assessments such as a Privacy and Civil Liberties Impact Assessment (PCLIA), IT system security assessments, technical quality reviews, and risk of bias assessments. The AI project team must complete all required approvals. For PCLIA requirements, see *IRM 10.5.2.2*, Privacy and Civil Liberties Impact Assessment (PCLIA).
d) The AI Governance PMO will compile all required artifacts and facilitate a review of the use case by the AI Assurance Team.
e) The AI Assurance Team will review all submitted artifacts, including applicable assessments from IT, PGLD, RAAS, or others, and assess the use case's readiness to be deployed in a production workflow. Subject Matter Experts (SMEs) in the AI Assurance Team will validate the project team's self-reported risk assessment for compliance with existing IRS policies relating to privacy, security, equity, etc.

f) The AI Assurance Team will provide a Readiness Assessment Report to the AI project team, AI Governance PMO, and DASIB.
g) The AI Governance PMO will compile the Readiness Assessment Report and related materials into a Project Summary Report for DASIB and facilitate DASIB review and adjudication of safety-impacting or rights-impacting use cases.
h) DASIB will give final approval for deployment to a production workflow of all safety-impacting or rights-impacting use cases. A use case will be considered approved if a majority of DASIB members vote in favor. The AI Governance PMO will capture, document, and archive DASIB members' votes.
i) The AI Governance PMO will archive all submitted reports and artifacts.

(3) For use cases that have previously been approved for use in a production workflow, AI project teams must review their use case at least annually or when significant modifications are made to the AI use case and submit updated information to the AI Governance PMO for AI governance review. Continued monitoring and evaluation along with regular reviews promotes effectiveness and mitigates risks.

a) The term "significant modification" is defined in *Exhibit 10.24.1-1*, Terms and Acronyms, and refers to an update to an AI use case that meaningfully alters its impact on rights or safety. This may include modifications to a use case's AI model(s), its underlying data, or the context of its use.
b) "Updated information" to be provided to the AI Governance PMO must include performance metrics (e.g., regarding accuracy or disparate impact).

(4) Any significant modifications to the AI use case must be reported promptly to the AI Governance PMO, who will work with the project team to facilitate completion of any actions required for continued use. The AI Governance PMO is responsible for ensuring these reviews are completed at least annually and for maintaining documentation of review completion.

10.24.1.6 (MM-DD-YYYY)
AI Sharing and Collaboration

(1) In coordination with the Department of Treasury, and subject to the considerations in this subsection, the IRS must share AI code, models, and data assets in a manner that facilitates reuse and collaboration Government-wide and with the public. (OMB M-24-10 Section 4(d))

(2) All IRS sharing and release of AI code, models, and datasets will be performed under the direction of the CDAO, in coordination with relevant AI governance stakeholders (see *IRM 10.24.1.5.1*, AI Governance Key Stakeholders and Responsibilities).

(3) All IRS sharing and release of AI code, models, and datasets must follow requirements in the *Privacy Act* and in *IRC 6103*, Confidentiality and Disclosure of Returns and Return Information. For questions about IRC 6103, IRS employees may contact Counsel members of the AI Assurance Team. For the Privacy Act, see *IRM*

10.5.6, Privacy Act.

10.24.1.6.1 (MM-DD-YYYY)
Sharing and Releasing AI Code and Models

(1) In coordination with the Department of Treasury, the IRS must proactively share custom-developed code for AI in active use, including models and model weights, and must release it as open-source software on a public repository, unless: (OMB M-24-10 Section 4(d)(i))

a) The sharing of the code is restricted by law or regulation, including patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulation, and Federal laws and regulations governing classified information;
b) The sharing of the code would create an identifiable risk to national security, confidentiality of Government information, individual privacy, or the rights or safety of the public;
c) The IRS is prevented by a contractual obligation from doing so; or
d) The sharing of the code would create an identifiable risk to IRS mission, programs, or operations, or to the stability, security, or integrity of IRS systems or personnel.

(2) The IRS should prioritize sharing custom-developed code, such as commonly used packages or functions, that has the greatest potential for re-use by other agencies or the public.(OMB M-24-10 Section 4(d)(i))

(3) For guidance and best practices related to sharing code and releasing it as open source, see *OMB Memorandum M-16-21*, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (Aug. 8, 2016). The IRS should also draw upon existing collaboration methods to facilitate the sharing and release of code and models, including the council described in Section 10.1(a) of Executive Order 14110, the General Services Administration's AI Community of Practice, and *https://www.code.gov*, as well as other publicly available code repositories. (OMB M-24-10 Section 4(d)(i))

(4) For IRS open source software (OSS) requirements, see *IRM 10.8.1*, Policy and Guidance.

10.24.1.6.2 (MM-DD-YYYY)
Sharing and Releasing AI Data Assets

(1) The following sharing and release requirements apply only to the extent that they do not conflict with requirements in the Privacy Act or IRC 6103. For questions about IRC 6103, IRS employees may contact Counsel representatives on the AI Assurance Team. For the Privacy Act, see *IRM 10.5.6*, Privacy Act.

(2) Data used to develop and test AI is likely to constitute a "data asset" for the purposes of implementing the Open, Public, Electronic and Necessary (OPEN) Government Data Act, and the IRS must, in coordination with the Department of

Treasury, release such data assets publicly as open government data assets if required by that Act and pursuant to safety and security considerations in Section 4.7 of Executive Order 14110. (OMB M-24-10 Section 4(d)(ii))

(3) Where such data is already publicly available, the IRS is not required to duplicate it, but should maintain and share the provenance of such data and how others can access it. (OMB M-24-10 Section 4(d)(ii)).

10.24.1.6.3 (MM-DD-YYYY)
Partial Sharing and Release

(1) Where some portion of an AI project's code, models, or data cannot be shared or released publicly pursuant to *IRM 10.24.1.6.1*, Sharing and Releasing AI Code and Models, and *IRM 10.24.1.6.2*, Sharing and Releasing AI Data Assets, the rest must still be shared or released where practicable, such as by releasing the data used to evaluate a model even if the model itself cannot be safely released, or sharing a model within the Federal Government even if it cannot be publicly released. (OMB M-24-10 Section 4(d)(iii)) Data sharing helps to address data scarcity challenges.

(2) Where code, models, or data cannot be released without restrictions on who can access it, the IRS should also, where practicable, share them through federally controlled infrastructure that allows controlled access by entities outside the Federal Government, such as via the National AI Research Resource. (OMB M-24-10 Section 4(d)(iii))

(3) All sharing must follow legal requirements related to disclosure, and any sharing of PII, Federal Tax Information (FTI), or other sensitive information should be coordinated via a Memorandum of Understanding (MOU) or similar agreement that outlines requirements and limitations.

10.24.1.6.4 (MM-DD-YYYY)
Procuring AI for Sharing and Release

(1) To the extent practicable and compliant with legal requirements such as those in the Privacy Act and IRC 6103, when procuring custom-developed code for AI, data to train and test AI, and enrichments to existing data (such as labelling services), the IRS should do so in a manner that allows for the sharing and public release of the relevant code, models, and data. (OMB M-24-10 Section 4(d)(iv))

(2) Acquisition teams must ensure that a Federal Acquisition Regulation (FAR) rights in data clause providing for appropriate rights to custom-developed code is included in the contract (see *FAR Subpart 27.4*, Rights in Data and Copyrights). Additionally, the contract should require delivery of source code, models, data, and documentation to the IRS.

10.24.1.6.5 (MM-DD-YYYY)
Unintended Disclosure of Data from AI Models

(1) When deciding whether to share and release AI models and model weights, the IRS must assess the risk that the models can be induced to reveal sensitive details of the data used to develop them. IRS assessment of risk should include a model-specific risk analysis. (OMB M-24-10 Section 4(d)(v))

10.24.1.7 (MM-DD-YYYY)
Determining Whether AI is Safety-Impacting or Rights-Impacting

(1) In accordance with OMB guidance, the IRS will review each AI use case to determine whether it matches the definition of safety-impacting or rights-impacting AI. (OMB M-24-10 Section 5(b)) Stakeholders such as the AI Governance PMO, AI Assurance Team, DASIB, and RAIO will support the Treasury CAIO in making this determination.

(2) AI used for a purpose identified by OMB as presumed safety-impacting or rights-impacting will be considered safety-impacting or rights-impacting unless a context-specific and system-specific risk assessment is conducted and the Treasury CAIO, in coordination with other relevant officials such as the IRS RAIO, determines that the AI use case does not match the definition of safety-impacting or rights-impacting and therefore is not subject to the minimum practices for safety-impacting or rights-impacting use cases. (OMB M-24-10 Section 5(b))

10.24.1.8 (MM-DD-YYYY)
Minimum Practices Before and During Use of Safety-Impacting or Rights-Impacting AI

(1) In accordance with OMB guidance, by December 1, 2024, the IRS must follow the minimum practices for safety-impacting or rights-impacting AI outlined in this section, or else stop using any AI that is not compliant with the minimum practices, consistent with the details and caveats in this subsection. (OMB M-24-10 Section 5(c))

(2) The IRS must document their implementation of these practices and be prepared to report them either as a part of the annual AI use case inventory, during periodic accountability reviews, or upon request. (OMB M-24-10 Section 5(c))

(3) The IRS will not be required to follow the minimum practices outlined in this subsection when using AI solely for one or more of the following purposes: (OMB M-24-10 Section 5(c)(i))

a) Evaluation of a potential vendor, commercial capability, or freely available AI capability that is not otherwise used in agency operations, exclusively for the purpose of making a procurement or acquisition decision.

Note: Those making procurement or acquisition decisions must follow existing procurement policies and ensure potential AI bias toward vendors is mitigated, even if the AI used to evaluate vendors or capabilities is exempt from the minimum practices in this subsection.

b) Achieving conformity with the requirements of this subsection, such as using an AI application in controlled testing conditions to carry out the minimum testing requirements below.

Note: AI used for this purpose must still follow relevant IRS and Treasury policies, such as those related to testing with sensitive data.

(4) The IRS, in coordination with the Treasury CAIO, may request from OMB an extension of up to one year for a particular use of AI that cannot feasibly meet the minimum requirements in this section by OMB's implementation deadline (December 1, 2024). OMB will not grant renewals beyond the initial one-year extension. Any extension request must be submitted prior to October 15, 2024, and include: (OMB M-24-10 Section 5(c)(ii))

a) A detailed justification for why the IRS cannot achieve compliance for the use case in question;
b) An explanation of practices the IRS has in place to mitigate the risks from noncompliance; and
c) A plan for how the IRS will come to implement the full set of required minimum practices from this subsection.

(5) In coordination with relevant IRS officials such as the RAIO, the Treasury CAIO may waive one or more of the requirements in this subsection for a specific covered AI use case after making a written determination, based upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. The Treasury CAIO may revoke a previously issued waiver at any time. (OMB M-24-10 Section 5(c)(iii))

10.24.1.8.1 (MM-DD-YYYY)
AI Impact Assessment

(1) Before using safety-impacting or rights-impacting AI, the IRS must complete an AI impact assessment. This impact assessment should be updated periodically and leveraged throughout the AI use case's lifecycle. The impact assessment must document at least the following: (OMB M-24-10 Section 5(c)(iv)(A))

a) The intended purpose for the AI and its expected benefit, supported by specific metrics or qualitative analysis.
b) The potential risks of using AI, along with any mitigation measures beyond these minimum practices that the IRS will take to help reduce these risks.
c) The quality and appropriateness of the relevant data.

10.24.1.8.2 (MM-DD-YYYY)
Real-World Performance Testing

(1) Before using safety-impacting or rights-impacting AI, the IRS must conduct adequate testing to ensure the AI, as well as components that rely on it, will work in its intended real-world context. Such testing should follow domain-specific best practices, when available, and should consider both the specific technology used and feedback from human operators, reviewers, employees, and customers who use the service or are impacted by the system's outcomes. Testing conditions should mirror as closely as possible the conditions in which the AI will be deployed. Test results should demonstrate that the AI will achieve its expected benefits and that associated risks will be sufficiently mitigated. (OMB M-24-10 Section 5(c)(iv)(B))

10.24.1.8.3 (MM-DD-YYYY)
Independent Evaluations

(1) Before using safety-impacting or rights-impacting AI, the IRS must review relevant AI documentation to ensure that the use case works appropriately and as intended, and that its expected benefits outweigh its potential risks. At a minimum, this documentation must include the completed impact assessment and results from testing AI performance in a real-world context (see *IRM 10.24.1.8.1*, AI Impact Assessment, and *IRM 10.24.1.8.2,* Real-World Performance Testing). (OMB M-24-10 Section 5(c)(iv)(C))

(2) The IRS will meet this requirement via the AI governance process described in *IRM 10.24.1.5.3*, AI Governance Process for AI Use Cases, and will follow all Treasury governance process requirements.

10.24.1.8.4 (MM-DD-YYYY)
Ongoing Monitoring and Risk Evaluation

(1) The IRS must institute ongoing procedures to monitor degradation of the AI's functionality and to detect changes in the AI's impact on rights and safety. This monitoring process must include periodic human reviews to determine whether the deployment context, risks, benefits, or IRS needs have evolved. The IRS must also determine whether the current implementation of these minimum practices adequately mitigates new and existing risks, or whether updated risk response options are required. (OMB M-24-10 Section 5(c)(iv)(D))

(2) At a minimum, human review is required at least on an annual basis and after significant modifications to the AI or to the conditions or context in which the AI is used, and the review must include renewed testing for performance of the AI in a real-world context. Reviews must also include oversight and consideration by an appropriate internal authority not directly involved in the system's development or operation. (OMB M-24-10 Section 5(c)(iv)(E))

(3) Contracts for safety-impacting or rights-impacting AI should include Quality Assurance Surveillance Plan (QASP) language providing the legal right for government personnel or support contractors to perform independent evaluations or inspections of

contractor AI systems (see *FAR Part 46*, Quality Assurance).

(4) The IRS will document compliance with these monitoring and evaluation requirements via the AI Governance process outlined in *IRM 10.24.1.5.3,* AI Governance Process for AI Use Cases.

10.24.1.8.5 (MM-DD-YYYY)
Emerging Risk Mitigation

(1) Upon identifying new or significantly altered risks to rights or safety through continuous monitoring, periodic review, or other mechanisms, the IRS must take steps to mitigate those risks, including, as appropriate, through updating the AI to reduce its risks or implementing procedural or manual mitigations, such as more stringent human intervention requirements. (OMB M-24-10 Section 5(c)(iv)(F))

(2) As significant modifications make the existing implementation of the other minimum practices in this subsection less effective, such as by making training or documentation inaccurate, the IRS must update or repeat those practices, as appropriate. (OMB M-24-10 Section 5(c)(iv)(F))

(3) Where the AI's risks to rights or safety exceed an acceptable level and where mitigation strategies do not sufficiently reduce risk, the IRS must stop using the AI as soon as is practicable. (OMB M-24-10 Section 5(c)(iv)(F))

10.24.1.8.6 (MM-DD-YYYY)
Human Training and Assessment

(1) The IRS must ensure there is sufficient training, assessment, and oversight for operators of the AI to interpret and act on the AI's output (if applicable), combat any human-machine teaming issues (such as automation bias), and ensure the human-based parts of the system effectively manage risks from the use of AI. Training should be conducted on a periodic basis, determined by the agency, and should be specific to the AI use case, product, or service being operated and how it is being used. (OMB M-24-10 Section 5(c)(iv)(G)) Ensuring ethical compliance and addressing unforeseen scenarios are also important cases for human training.

10.24.1.8.7 (MM-DD-YYYY)
Human Oversight of Decisions or Actions

(1) The IRS must assess its safety-impacting or rights-impacting use cases to identify any decisions or actions in which the AI is not permitted to act without additional human oversight, intervention, and accountability. When immediate human intervention is not practicable for such an action or decision, the IRS must ensure that the AI functionality has an appropriate fail-safe that minimizes the risk of significant harm. (OMB M-24-10 Section 5(c)(iv)(H))

(2) The IRS will assess safety-impacting or rights-impacting use cases and ensure

compliance with this requirement through the AI Governance process outlined in *IRM 10.24.1.5.3*, AI Governance Process for AI Use Cases.

10.24.1.8.8 (MM-DD-YYYY)
Public Notice and Plain Language Documentation

(1) The IRS must ensure that each entry in the AI use case inventory of a use case that is safety-impacting or rights-impacting provides accessible documentation of the use case's functionality in plain language. To the extent consistent with applicable law and government-wide guidance, including those concerning protection of privacy and of sensitive law enforcement, national security, and other protected information, these entries will serve as public notice of the AI to its users and the general public. (OMB M-24-10 Section 5(c)(iv)(I)) See *IRM 10.24.1.4,* AI Use Case Inventory.

(2) Where people interact with a service relying on the AI and are likely to be impacted by the AI, the IRS must provide reasonable and timely notice about the use of the AI and a means to directly access the documentation about it in the use case inventory. (OMB M-24-10 Section 5(c)(iv)(I))

(3) Where IRS use cases are not included in the public AI use case inventory, they may still be required to report relevant information to OMB and must ensure adequate transparency in their use of AI, as appropriate and consistent with applicable law. (OMB M-24-10 Section 5(c)(iv)(I)) The AI Governance PMO, under the direction of the CDAO, will be responsible for coordinating required reporting.

Note: A System of Records Notice (SORN) or Privacy and Civil Liberties Impact Assessment (PCLIA) may also be used to help ensure adequate transparency and protection of privacy. See *IRM 10.5.2.2*, Privacy and Civil Liberties Impact Assessment, and *IRM 10.5.6.3*, Privacy Act System of Records Notices (SORNs).

10.24.1.8.9 (MM-DD-YYYY)
Equity and Fairness

(1) Before initiating use of any rights-impacting AI, the IRS must take steps to identify and assess the AI's impact on equity and fairness, and mitigate algorithmic discrimination when it is present. The IRS must: (OMB M-24-10 Section 5(c)(v)(A))

a) Identify and document in their AI impact assessment when using data that contains information about a class protected by federal nondiscrimination laws (e.g., race, age, etc.). Given the risks arising when AI may correlate demographic information with other types of information, the IRS should also assess and document whether the AI model could foreseeably use other attributes as proxies for a protected characteristic and whether such use would significantly influence model performance;
b) Assess the AI in a real-world context to determine whether the AI model results in significant disparities in the model's performance (e.g., accuracy, precision, reliability

in predicting outcomes) across demographic groups;

c) Mitigate disparities that lead to, or perpetuate, unlawful discrimination or harmful bias, or that decrease equity as a result of the IRS's use of the AI; and

d) Cease use of the AI for IRS decision-making, consistent with applicable law, if the IRS is unable to adequately mitigate any associated risk of unlawful discrimination against protected classes. The IRS should maintain appropriate documentation to go with this decision-making, and should disclose it publicly to the extent consistent with applicable law and government-wide policy.

Note: Documentation may include a PCLIA. See *IRM 10.5.2.2*, Privacy and Civil Liberties Impact Assessment (PCLIA).

10.24.1.8.10 (MM-DD-YYYY)
Incorporation of Feedback

(1) Before initiating use of any rights-impacting AI and consistent with applicable law and government-wide guidance, the IRS must consult affected communities, including underserved communities, and request public feedback, where appropriate, in the design, development, and use of the AI. The IRS must use such feedback to inform their decision-making regarding the AI. The consultation and feedback process must include seeking input on the IRS's approach to implementing the minimum risk management practices established in this subsection, such as applicable opt-out procedures. The IRS should consider and manage the risks of public consultation in contexts like fraud prevention and law enforcement investigations, where consulting with the targeted individual is impractical but consulting with a representative group may be appropriate. (OMB M-24-10 Section 5(c)(v)(B))

10.24.1.8.11 (MM-DD-YYYY)
Ongoing Monitoring and Mitigation for AI-enabled Discrimination

(1) As part of the ongoing monitoring requirement in *IRM 10.24.1.8.4*, Ongoing Monitoring and Risk Evaluation, the IRS must also monitor rights-impacting AI to specifically assess and mitigate AI-enabled discrimination against protected classes, including discrimination that might arise from unforeseen circumstances, changes to the system after deployment, or changes to the context of use or associated data. Where sufficient mitigation is not possible, the IRS must safely discontinue use of the affected AI functionality. (OMB M-24-10 Section 5(c)(v)(C))

10.24.1.8.12 (MM-DD-YYYY)
Notification of Negatively Affected Individuals

(1) Consistent with applicable law and government-wide guidance, when using rights-impacting AI the IRS must notify individuals when use of the AI results in an adverse decision or action that specifically concerns them, such as the denial of benefits or deeming a transaction fraudulent. The notice must also include a clear and accessible

means of contacting the IRS and, where applicable, provide information to the individual on their right to appeal. (OMB M-24-10 Section 5(c)(v)(D)) See also *IRM 10.5.1.3.2.9*, Access, Correction, and Redress.

10.24.1.8.13 (MM-DD-YYYY)
Human Consideration and Remedy Processes

(1) Where practicable, appropriate, and consistent with applicable law and government-wide guidance, when using rights-impacting AI the IRS must provide timely human consideration and potential remedy to the use of the AI via a fallback and escalation system in the event that an impacted individual would like to appeal or contest the AI's negative impacts on them. The IRS may leverage or expand existing appeals and/or secondary human review processes to meet this requirement. (OMB M-24-10 Section 5(c)(v)(E))

(2) In seeking to meet this requirement, IRS business units or offices using AI must not assume that the Independent Office of Appeals will be the first finders of fact in cases where individuals would like to appeal or contest the impacts of IRS AI use. Instead, IRS business units or offices using AI must develop and maintain internal review processes to resolve issues or disputes that arise. If a controversy or dispute remains after internal review, then referral to Appeals may be appropriate.

(3) When the IRS is unable to provide an opportunity for an individual to appeal due to law, government-wide guidance, or impracticability, the IRS must create appropriate alternative mechanisms for human oversight of the rights-impacting AI. (OMB M-24-10 Section 5(c)(v)(E))

10.24.1.8.14 (MM-DD-YYYY)
Opt Out Options

(1) Where practicable and consistent with applicable law and government-wide guidance, when using rights-impacting AI the IRS must provide and maintain a mechanism for individuals to conveniently opt out from AI functionality in favor of a human alternative. An opt-out mechanism must be prominent, readily available, and accessible, and it is especially critical where the affected people have a reasonable expectation of an alternative or where lack of an alternative would meaningfully limit availability of a service or create unwarranted harmful impacts. (OMB M-24-10 Section 5(c)(v)(F)) See also *IRM 10.5.1.3.2.4*, Openness and Consent.

(2) The IRS is not required to provide the ability to opt out if the AI functionality is solely used for the prevention, detection, and investigation of fraud or cybersecurity incidents, or the conduct of a criminal investigation. The Treasury CAIO may waive the opt-out requirement if the IRS can demonstrate that a human alternative would result in a service that is less fair (e.g., produces a disparate impact on protected classes) or if an opt-out would impose undue hardship on the IRS. (OMB M-24-10 Section 5(c)(v)(F))

10.24.1.9 (MM-DD-YYYY)

Ethical Standards and Protection of Taxpayer Rights

(1) The IRS must ensure that AI solutions are guided by ethical standards that emphasize the protection and prioritization of taxpayer rights. (EO 14110 Section 2(a))

(2) The IRC lists specific taxpayer rights (see *IRC 7803(a)(3)*) which are further explained in The Taxpayer Bill of Rights (see *Pub 1*, Your Rights as a Taxpayer, and *www.irs.gov/taxpayer-bill-of-rights*). 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 (MM-DD-YYYY)
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) In particular, those developing, procuring, or using AI must follow requirements in these IRM subsections when they apply:

a) *IRM 10.5.2.2*, Privacy and Civil Liberties Impact Assessment (PCLIA).

Note: For an explanation of civil liberties, see *IRM 10.5.2.2.2.1*, Civil Liberties.

b) *IRM 10.5.6.3*, Privacy Act System of Records Notices (SORNs).
c) *IRM 10.5.6.5*, Privacy Act Recordkeeping Restrictions (Civil Liberties Protections).

Exhibit 10.24.1-1 (MM-DD-YYYY)
Terms and Acronyms

Term	Definition
Accessibility	The term “accessibility” has the meaning provided in Section 2(e) of *Executive Order 14035*.
Algorithmic Discrimination	The term “algorithmic discrimination” has the meaning provided in Section 10(f) of *Executive Order 14091*.

Artificial Intelligence (AI)	In accordance with OMB M-24-10 Section 6, 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 (NDAA), which states that “the term ‘artificial intelligence’ includes the following”: 1) 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. 2) 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. 3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. 4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. 5) 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. OMB M-24-10 Section 6 provides the following additional guidance regarding the NDAA definition of AI: 1) This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including, but not limited to, deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI. 2) 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. 3) For this definition, no system should be considered too simple to qualify as a covered AI system 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). 4) 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.

AI Maturity	In accordance with OMB M-24-10 Section 6, the term “AI maturity” refers to a Federal Government organization’s capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with relevant federal law, regulation, and policy on AI.
AI Model	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. (EO 14110 Section 3(c)) Put simply, an AI model is the specific set of AI methods used to carry out the objective of the use case, e.g., a large language model.
AI Red-Teaming	The term “AI red-teaming” has the meaning provided for “AI red-teaming” in Section 3(d) of *Executive Order 14110*.
AI Use Case	A specific business use for AI, e.g., to solve a problem or increase operational efficiency. Includes outcomes or impact. May use one or more models to achieve its objective(s).
Automation Bias	The term “automation bias” refers to the propensity for humans to inordinately favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.
BOD	Business Operating Division.
Chief Data and Analytics Officer (CDAO)	Refer to *IRM 1.1.18.1*, Research, Applied Analytics and Statistics Division, for a detailed description of responsibilities.
Chief Information Officer (CIO)/Chief Technology Officer (CTO)	Refer to *IRM 10.8.2*, IT Security Roles and Responsibilities, for a detailed description of responsibilities.
Counsel	Office of Chief Counsel.
Custom-Developed Code	The term “custom-developed code” has the meaning provided in Appendix A of *OMB Memorandum M-16-21*.
Cybersecurity and Infrastructure Security Agency (CISA)	An operational part of the Department of Homeland Security (DHS) that works to understand, manage, and mitigate risk to the nation’s cyber and physical infrastructure in the public and private sector.
DASIB	Data and Analytics Strategic Integration Board.
Data Asset	The term “data asset” has the meaning provided in *44 USC 3502*.

Dual-Use Foundation Model	The term “dual-use foundation model” has the meaning provided in Section 3(k) of *Executive Order 14110*.
EO	Executive Order.
Equity	The term “equity” has the meaning provided in Section 10(a) of *Executive Order 14091*.
FAR	Federal Acquisition Regulation.
Federal Information	The term “federal information” has the meaning provided in *OMB Circular A-130*: information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.
FISMA	Federal Information Security Management Act.
FOIA	Freedom of Information Act.
FTI	Federal Tax Information.
Generative AI	A 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.
GSA	General Services Administration.
IRA	Inflation Reduction Act.
IRA SOP	Inflation Reduction Act Strategic Operating Plan.
IRM	Internal Revenue Manual.
IT	Information Technology.
Model Weight	The term “model weight” has the meaning provided in Section 3(u) of *Executive Order 14110*.
MOU	Memorandum of Understanding.
NAAI	National Artificial Intelligence Initiative.
NARA	National Archives and Records Administration.
NDAA	National Defense Authorization Act.
NIST	National Institute of Standards and Technology.
NIST AI RMF	National Institute of Standards and Technology Artificial Intelligence Risk Management Framework.

OMB	Office of Management and Budget.
OPEN	Open, Public, Electronic and Necessary.
PCLIA	Privacy and Civil Liberties Impact Assessment.
PGLD	Privacy, Governmental Liaison, and Disclosure.
PMO	Project Management Office.
QASP	Quality Assurance Surveillance Plan.
RAAS	Research, Applied Analytics and Statistics.
Rights-Impacting AI	In accordance with OMB M-24-10 Section 6, the term “rights-impacting AI” refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect on that individual’s or entity’s: 1) Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance; 2) Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or 3) Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services. See OMB M-24-10 Appendix I(2) for a list of AI use case purposes which are presumed to be rights-impacting.
Responsible Artificial Intelligence Official (RAIO)	At the IRS, the CDAO is designated as RAIO. This designation follows EO 13960 Section 8(c), which directs agencies to appoint a "responsible [AI] official(s) at that agency," and with 2022 OMB guidance titled Suggested Practices for Assessing Agency AI Use Case Inventory, per EO 13960.

Safety-Impacting AI	In accordance with OMB M-24-10 Section 6, the term "safety-impacting AI" refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of: 1) Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms; 2) Climate or environment, including irreversible or significant environmental damage; 3) Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21 or any successor directive and the infrastructure for voting and protecting the integrity of elections; or, 4) Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government. See OMB M-24-10 Appendix I(1)for a list of AI use case purposes which are presumed to be safety-impacting.
Significant Modification	In accordance with OMB M-24-10 Section 6, the term "significant modification" refers to an update to an AI application or to the conditions or context in which it is used that meaningfully alters the AI's impact on rights or safety, such as through changing its functionality, underlying structure, or performance such that prior evaluations, training, or documentation become misleading to users, overseers, or individuals affected by the system. This includes significantly changing the context, scope, or intended purpose in which the AI is used.
SME	Subject Matter Expert.
Underserved Communities	The term "underserved communities" has the meaning provided in Section 10(b) of *Executive Order 14091*.

Exhibit 10.24.1-2 (MM-DD-YYYY)
Related Resources

Executive Orders

- *Executive Order 13960*, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government
- *Executive Order 14110*, Safe, Secure, and Trustworthy Development and Use of

Artificial Intelligence

IRS Publications

- *IRM 1.7.1*, Servicewide Research for Tax Administration
- *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*, Policy and Guidance
- *IRM 10.8.2*, IT Security Roles and Responsibilities
- *Pub 1*, Your Rights as a Taxpayer

Other Publications

- *OMB Memorandum M-24-10*, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence
- *OMB Memorandum M-16-21*, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software