DEPARTMENT OF THE TREASURY'S COMPLIANCE PLAN FOR OMB MEMORANDA M-24-10

September 2024

- Prepared by Todd Conklin, Chief AI Officer
- Issued by Adewale Adeyemo, Deputy Secretary of the Treasury

1. STRENGTHENING AI GOVERNANCE

I. <u>General</u>

A. Department of the Treasury ("Treasury") has stood up, and continues to stand up, multiple artificial intelligence (AI) related bodies. These include not only the OMB M-24-10 required AI Governance Board, chaired by the Deputy Secretary, but also:

1) An AI Working Group to address operational AI developments and implementation.

2) An AI Acquisitions Working Group to better coordinate and collaborate on AI system acquisition based on OMB guidance.

3) Multiple bureau and sub-component level AI bodies to allow for internal tactical coordination on AI use. This is being recommended to all bureaus and sub-components as capabilities allow.

4) Communication mechanisms for ensuring a bilateral flow of information across all AI related governance bodies. These mechanisms allow the AI Governance Board to have greater insight and visibility into the usage and development of AI across the entire Department, while also facilitating the flow of strategic guidance from the AI Governance Board to the sub-components.

5) An AI leadership group specifically focusing on leveraging AI to combat fraud both resulting in improper payments made by the and in support of the broader financial sector.

B. Treasury is in the process of reviewing individual sub-component AI use policies and procedures, as well as IT use policies and procedures. In addition to this, Treasury is developing an internal department-wide AI use policy and working with Treasury Bureaus to develop AI user agreements.

C. Treasury has been working closely with both U.S. Government entities and private

sector AI practitioners to gather a broad knowledge base of AI use best practices to include in any future policy or governance development.

II. <u>AI Governance Bodies</u>

A. The Treasury AI Governance Board is currently made up of the following officials or senior representatives from their offices:

1) Deputy Secretary of the Treasury (Chairperson)

2) Chief Artificial Intelligence Officer (Vice Chairperson)

3) Chief Information Officer (Co-Vice Chairperson)

4) Assistant Secretary for Financial Institutions

5) Assistant Secretary for Management / Senior Agency Official for Privacy / Head of Contracting Activity (HCA)

6) Fiscal Assistant Secretary

7) Financial Crimes Enforcement Director

8) IRS Chief Data and Analytics Officer / AI Responsible Official

9) Treasury Statistical Official

10) Chief Diversity, Equity, Inclusion, and Accessibility (DEIA) Officer

11) General Counsel

12) Chief Risk Officer / Deputy Performance Improvement Officer

13) Chief Data Officer

B. The AI Governance Board shall provide strategic leadership for Treasury's AI activities for safe and responsible adoption and use. The AI Governance Board's make up and role will ensure participation at the most senior levels within Treasury and drawing from essential offices and necessary backgrounds in all oversight, planning, and advancement of the usage of AI within the Department. The AI Governance Board will accomplish this through multiple objectives and responsibilities to include:

1) Establish an overall governance model and strategy for the use of AI within Treasury, including the setting of priorities for the effective and safe use of AI.

2) Guide the prioritization and implementation of initiatives to meet the AI related goals defined in EO 14110, OMB M-24-10, other relative directives, and the Treasury Strategic Plan.

3) Provide strategic guidance to Treasury offices and bureaus on AI policy priorities.

4) Review and approve Treasury's AI risk assessment/management framework as needed to reflect new guidance and developments.

5) Evaluate Treasury's highest risk AI use cases and attendant risk management strategies.

6) Identify the need for, and establish, any working groups, sub-committees, or

task forces to support M-24-10 related efforts, as well as additional priorities identified by the AI Governance Board.

       7) Continuously review and update policies in response to emerging risks and technological changes. This will be done in close coordination between the AI Governance Board and other relevant department officials.

C. Treasury has already begun to coordinate and interact with other AI professionals, specifically from other U.S. Government entities for the purpose of facilitating information sharing, and the adoption of best practices.

D. Treasury has also held small-scale meetings with academia and industry on AI governance and policy related topics for the purpose of increasing knowledge and awareness on AI related topics. As Treasury's AI governance practices, and overall usage of AI technologies mature, it is anticipated that the frequency of these meetings will increase.

III.   <u>AI Use Case Inventories</u>

A. Treasury has developed a portal where offices, bureaus, and sub-components will be able to upload information on their use case inventory. Designated representatives responsible for their respective sub-component's AI based technologies and automations will be tasked with completing, submitting, and updating (as necessary) a reporting form that describes and inventories their AI use cases. This internal Treasury form will be used until OMB finalizes a federal-wide format.

B. Members of an internal working group will initially review all reported use cases for completeness and items requiring further review will be flagged.

C. A separate subgroup will provide secondary use case review focusing on conducting a risk review/assessment on the use case to ensure that it does not violate requirements of safe and responsible use as set forth in EO 14110, OMB M-24-10 and other relevant OMB requirements. This sub-group will be made up of individuals representing risk, privacy, and data focused individuals.

       1) In instances where Treasury bureaus or components already have a review process in place that has been approved by the CAIO, these reviews will be done internally by the bureau or component with results provided to the AI Board. Sample sets of these internal reviews may be required to go through a secondary review by the above-mentioned subgroup to ensure oversight and compliance with OMB requirements.

D. Following the risk review process (further explained in Section 3 of this report) approved use cases will then be inventoried and posted to the treasury.gov/ai webpage for public viewing.

E. Treasury intends to update the use case inventory on a rolling and continuous basis as use cases are submitted. In situations where this is not possible, exceptions may be granted by the CAIO to allow use cases to be updated less frequently, but still at least annually, in accordance with OMB M-24-10. Additionally, existing use cases will be periodically reviewed and updated as needed.

IV.   <u>Reporting on AI Use Cases Not Subject to Inventory</u>

A. As part of the previously mentioned AI use case inventory collection and review, part

of the review process will include making the determination if the reported AI use case is not subject to inventory.

 B. This determination will be made by the previously mentioned sub-group made up of risk, privacy, and data focused individuals. Based on their review either a recommendation to inventory or not inventory will be made to the AI Governance Board.

 C. Based on this recommendation, the AI Governance Board members will discuss the request and make a final determination based on the criteria in OMB M-24-10.

 D. Treasury will still, on an annual basis, report and release aggregate metrics of these use cases that are otherwise in scope of M-24-10, the number of such cases that impact rights and safety, and their compliance with the practices of Section 5(c) of M-24-10, as is required by OMB.

 E. Periodically (at least annually), a sample of these excluded use cases will be reviewed by the same sub-group to identify any changes or updates. These cases will still be compared against the criteria in OMB M-24-10 and if any details of the use case change that no longer make it applicable for exclusion, the public use case inventory will be updated.

2. ADVANCING RESPONSIBLE AI INNOVATION

 I. <u>Removing Barriers to the Responsible Use of AI</u>

  A. Treasury continues to research and attempt to identify barriers to responsible use of AI. Current barriers that have been identified include limited understanding of AI systems and ambiguity in federal guidance on use and acceptable systems. To address and remove these barriers Treasury is looking to implement the following solutions.

   a. **Limited Understanding of AI Systems** – Refer to Section II below on AI Talent and Training.

   b. **Ambiguity in Federal Guidance -** As the definitions of covered and non-covered AI use cases continue to change since the publication of M-24-10 and guidance on what systems are considered AI and what systems are not considered AI continues to change, Treasury is in the process of developing an AI acceptable use policy and an AI user agreement. These policies are intended to serve as documents that can provide guidance and clarity to Treasury employees until consistent and clarified guidance can be provided by OMB and other Federal Sources.

 II. <u>AI Talent and Training</u>

  A. Treasury has begun working with the General Services Administration (GSA) to acquire training developed by GSA. This training is expected to be embedded into Treasury's employee learning platform by the end of Calendar Year 2024. This training is planned to exist in four different tracks. These tracks would include:

   1) General User Training – this training will be an introductory training curriculum that would be required for all AI system users in Treasury as well as offered as an optional training for all other Treasury employees.

2) Technology – this training would be required for all Treasury employees that will be maintaining or providing technical activities for AI systems as well as offered as optional training for all other Treasury employees.

3) Acquisitions – this training will be required for all Treasury employees involved in AI system acquisition as well as optional training for all other Treasury employees.

4) Leadership – this training will be required for all Treasury employees who will be supervising or managing teams or employees who will be AI system users as well as optional training for all other Treasury employees.

B. Treasury is also encouraging employees to leverage existing no-cost AI training courses such as GSA's Center of Excellence AI Training Series, free open-source AI training videos, and existing AI related trainings found in FedVTC to supplement AI training.

III. AI Sharing and Collaboration

A. Treasury is committed to sharing and collaborating across the Federal Government regarding AI use cases, systems, and codes.

   i. Any AI code developed by Treasury will leverage the AI Governance Board as the mechanism for sharing when reasonable and not subject to exemption from public disclosure, in alignment with OMB M-24-10(4)(d). This would be done through CAIO and CIO interactions with other agencies through various committees and bodies currently in place across the federal landscape.

   ii. Publication of AI use cases to the public Treasury.gov/ai website will also allow for use case details and information to be shared with Federal Government partners. Treasury will ensure transparent communication with other Federal D/As that have an interest in existing use cases or active models and systems within Treasury.

B. Treasury has always had a strong partnership with private sector partners. The sharing of AI models, systems, and codes will be no different. However, Treasury understands that there will be certain models, systems, and code that have law enforcement applications and will not be suitable for sharing or may only be shared in generic forms.

   i. In support of this, Treasury is committed to encouraging and supporting employees to attend, present at, and engage with, leading tech conferences in AI to foster collaboration, learning, and innovation.

   ii. Treasury, through the relevant offices, will work to ensure that not only are AI use case inventories publicly posted, but that there is discussion with the private sector on models and code currently in use when feasible.

   iii. These conversations will likely occur through numerous offices and bureaus as each component of Treasury has different public-private relationships.

   iv. Additionally, Treasury will work through the Public Affairs office to ensure that relevant information is shared with the public on AI models and systems in use at Treasury.

IV. Harmonization of Artificial Intelligence Requirements

A. Treasury is committed to sharing best practices across the Department and across the Federal Landscape.

   i. Treasury has established an internal SharePoint page which will be used to host information regarding best practices in the AI space. This includes sharing documentation on approaches to risk management, roll-out roadmaps, and policy and governance strategies. As this page is built out, offices, bureaus, and components of Treasury will be able to share and exchange their lessons learned in a centralized location.

   ii. The AI Governance Board is also serving as a venue to share and document best practices and lessons learned. Members of the AI Governance Board have held multiple meetings with interagency partners and even private sector partners to exchange ideas and information related to how organizations are addressing risk concern, user policies, and implementation/roll-out strategies.

   iii. Treasury has also participated in, and will continue to participate in, requests for information, public inputs, and interagency exercises focused on AI use, implementation, innovation, risk identification, and incident response. These exercises, public inputs, and requests for information, allow Treasury to not only share knowledge and lessons learned but also allow Treasury to learn from other organizations facing similar challenges and opportunities.

3. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

I. <u>Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting</u>

   A. Treasury review of use cases will include case-by-case determinations whether each case is rights or safety-impacting based on the criteria set forth in Section 6 of M-24-10. This will be done through a review by a group focused on conducting risk assessments for all AI use cases. Specifically, the group will review if the use case will be used to make determinations or decisions that impact employee or public civil rights or liberties (in cases of rights-impacting) or if the use case will be used in a manner that may impact safety of the users, such as in automation processes of machinery (in cases of safety-impacting).

   ι. As with the initial use case risk review process, instances where Treasury bureaus or components already have a review process in place that has been approved by the CAIO, these reviews will be done internally by the bureau or component with results provided to the AI Board. Sample sets of these internal reviews may be required to go through a secondary review by the above-mentioned subgroup to ensure oversight and compliance with OMB requirements.

   B. In addition to M-24-10 guidance on rights and safety-impacting use case criteria, Treasury will also consider AI ethicist recommendations, best practices from other government agencies, and best practices and recommendations from outside the federal government when making determinations on potential rights or safety-

impacting AI systems.

    C. Treasury will use waivers as needed or determined necessary by the Chief AI Officer. The waiver process will include a thorough review of the use case submitted by the intended user. Following review of the use case, if a risk assessment determines the system to be rights or safety-impacting the intended user will be allowed an opportunity to provide a rationale for continued pursuit of the use case. This rationale will include mitigation steps to reduce the risk posed by the system as well as an explanation as to why this system should be allowed when compared to other potential alternate systems or through non-AI based means. Following this rationale, it will be further reviewed by the risk assessment group which will include risk management officials, privacy officials, diversity, equity, inclusion, and accessibility officials, and representatives from general counsel, at a minimum. Following their review a recommendation will be made to either deny or approve the waiver request. At this point the recommendation will be provided to the Chief AI Officer for final decision, in accordance with M-24-10. Details on the waiver will be maintained by the AI Governance Board and the granting of a waiver will be noted on the public use case inventory (if applicable) as well as provided to OMB for awareness. The waiver will be reviewed at least annually to ensure it is still necessary and valid. This review will be done by the system user and the risk assessment group with recommendations on continued approval or revocation being made to the Chief AI Officer.

II.   Potential Sources for Risk Review and Management Practices

    A. While not required by M-24-10, Treasury will be using additional resources to identify and manage potential risks posed by AI use.

    B. Treasury will consult audit recommendations that are published or shared from organizations, such as GAO, that address or focus on AI use risk identification, management, and mitigation.

    C. Treasury will also consider potential impacts from supply chain risks that are identified in AI software and system environments. This could include potential criteria such as ownership, data storage, and other factors.

III.   Implementation of Risk Management Practices and Termination of Non-Compliant AI

    A. Treasury is in the process of developing an acceptable use policy and user agreement. Within this policy, Treasury will outline the requirements to ensure that AI system use is compliant with OMB and Treasury directives. Part of this will include that responsible officials from each sub-component will provide certification that the AI systems being employed meet these requirements. This will ensure that rights or safety impacting AI systems that have not either been approved or granted a waiver are not used internally or by the public.

    B. Additionally, reviews will occur on a pre-determined basis to review use cases, documentation, and risk assessments to ensure that unauthorized AI systems are not being used within Treasury.

    C. Treasury has already begun the practice of limiting access to online-based AI systems to prevent unauthorized use of these systems until they have been reviewed and decided upon by the AI Governance Board.

    D. If rights or safety-impacting AI systems do appear on Treasury networks or infrastructure without prior approval, Treasury OCIO will work with the entities

involved to ensure that the AI systems are terminated and removed until a thorough review for compliance with OMB minimum requirements have been completed. Treasury will also investigate the unauthorized use or unauthorized system to determine what, if any, impact the use may have had on employees or the public. If necessary, potential punitive action(s) will be assessed and administered under applicable legal standards.

IV.   <u>Minimum Risk Management Practices</u>

A. Within Treasury's pending AI use policy, each sub-component will be instructed to identify a senior accountable official for AI use in the organizations. This may be the CIO, CTO, CAIO, or other knowledgeable senior official. These officials will be responsible for conducting internal review and validation to ensure that minimum risk practices are being implemented and maintained.

B. Treasury will also, through its risk assessment process, conduct regularly occurring risk assessments on all AI use cases. While this will focus on all AI use cases, there will be additional focus on those that have previously been identified as potentially rights or safety impacting, to ensure that risk management practices are being maintained and recertify the validity of any waivers or required mitigation practices.