EXIM Compliance Plan for OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance and Public Trust

July 2025

Version:2.0

Prepared by Howard Spira, Senior Vice President, CIO and Chief Artificial Intelligence Officer

REVISION HISTORY

Date	Name	Description of Change	Version
09/24/2024	AI Governance body	Initial Publication	1.0
07/25/2025	AI Governance Body	Reissued AI Compliance Plan per M-25-21 Supersedes AI Compliance Plan of September 2024	2.0

TABLE OF CONTENTS

PURPOSE

The Artificial Intelligence (AI) in Government Act of 2020[1] and OMB Memorandum M-25-21[2], *Accelerating Federal Use of AI through Innovation, Governance and Public Trust*, directs each agency to submit to the Office of Management and Budget (OMB) and post publicly on its website either a plan to achieve consistency with M-25-21 or a written statement that the agency does not use and does not anticipate using covered AI.

This document outlines the minimum information required for the Export-Import Bank of the United States (EXIM)'s compliance plans that will satisfy the requirements of Section 3(b)(ii) of the Appendix to OMB Memorandum M-25-21 and Section 104(c) of the AI in Government Act. EXIM will report compliance with the individual use-case-specific practices mandated in Section 4 of M-25-21 Appendix separately through the annual AI use case inventory.

AUTHORITY

The establishment of AI policies within EXIM is primarily guided by mandates from OMB, Presidential Directives, and other federal regulations. OMB mandates, such as the Federal Data Strategy, the Cloud Smart Strategy, and Accelerating Federal Use of AI through Innovation, Governance and Public Trust, provide a framework for leveraging data as a strategic asset and adopting modern technology practices, including AI. These authorities collectively empower federal agencies to develop and implement AI policies that align with national priorities, promote innovation, and maintaining the public trust in the use of AI technologies.

SCOPE

This AI Compliance plan applies to EXIM, including its employees and all third parties (such as consultants, vendors, and contractors) that use or access any information technology (IT) resources under the administrative responsibility of EXIM or its IT services. This encompasses systems managed or hosted by third parties on behalf of the agency.

This policy covers all technology systems that deploy AI technology, hereinafter called "AI systems." AI is a machine-based system that can make predictions, recommendations, or decisions influencing real or virtual environments for a given set of human-defined objectives. AI systems use machine and human-based inputs to perceive environments, abstract perceptions into models through automated analysis, and use model inference to formulate options for information or action. The definition includes systems using machine learning, large language models, natural language processing, computer vision technologies, and generative AI. It excludes basic calculations, basic automation, or pre-recorded "if this, then that" response systems.

[1] H.R.2575 - 116th Congress (2019-2020): AI in Government Act of 2020 | Congress.gov | Library of Congress

[2] M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

This policy applies to all new and existing AI systems developed, used, or procured by EXIM, which could directly impact the mission or security of EXIM.

ABOUT EXIM

EXIM is the official export credit agency of the United States with a mission of supporting American jobs by facilitating the export of U.S. goods and services. EXIM mitigates risk, backed by the full faith and credit of the United States, for American businesses by equipping them with the financing tools necessary to compete for global sales. In doing so, EXIM levels the playing field for U.S. goods and services going up against foreign competition in overseas markets.

EXIM is a small, independent agency. The preponderance of EXIM's technology capabilities are delivered with state-of-the-market commercial IT tools - commercial hardware, software, cloud services, and various data and service providers. EXIM performs relatively little custom systems development work. What custom development work the agency does perform focuses on low volume transaction processing applications that do not currently include AI capabilities. The agency's staff numbers approximately 300 federal team members based mainly in Washington DC.

DRIVING AI INNOVATION

EXIM is committed to fostering an environment where AI technologies can be used, developed, and deployed responsibly for the benefit of the Bank. Leveraging AI's potential to enhance our operations and ensuring that such advancements align with regulatory standards through the program described by this document is the foundation of EXIM's effort for accelerating AI use at EXIM.

The development of an AI strategy is important for EXIM to leverage AI's full potential while ensuring alignment with our mission, values, and regulatory requirements. EXIM is currently developing its AI strategy in concert with its other strategy processes and practices and expects to complete that work in FY26. EXIM's AI strategy will focus on integrating AI into our operations responsibly and effectively, driving innovation, and managing associated risks.

Removing Barriers to the Responsible Use of AI

One of EXIMs primary goals is to identify and mitigate barriers to the responsible use of AI. We have undertaken several initiatives to achieve this goal:

- **Barrier Identification:** Conduct reviews to identify barriers to AI adoption, including issues related to data access, technical infrastructure, and organizational readiness.

- **Mitigation Strategies:** Develop and implement strategies to address barriers, such as enhancing data governance frameworks, investing in AI infrastructure, and providing targeted staff training.
- **Resource Allocation:** Ensuring necessary resources, including staffing and budgetary resources, to support responsible AI use.

Currently, there are no explicit barriers to the responsible use of AI at EXIM. However, there are pressures that impact the adoption of any new capabilities that apply broadly and are not exclusive to AI:

- AI use cases compete for funding and staffing with other important priorities at the Bank including investments in core EXIM capabilities, cyber security, and other use cases in our modernization agenda.
- Planning processes to line up funding and staff resources that typically requires a budget cycle to implement significant new initiatives.

EXIM simultaneously has some advantages in the adoption of AI and currently has a posture that is relatively permissive with respect to adoption of non-safety, non-rights impacting AI:

- The agency deals predominantly with moderate sensitivity, open source, and commercially provided information. Many promising use cases at EXIM avoid safety and rights impacting domains, reducing barriers to implementation.
- The agency's technology is dominated by commercial off-the-shelf capabilities which are rapidly accreting useful AI as a natural extension of their capabilities.
- As a small agency, decision making is relatively nimble and speedy compared to larger organizations.

Currently EXIM is not experiencing any barriers with respect to its AI roadmap with access to the necessary software tools, open-source libraries, and deployment and monitoring capabilities to rapidly develop, test, and maintain AI applications as the current focus on AI is more oriented towards exploiting and taking advantage of AI features in commercial software and not the direct development of AI applications.

Sharing and Reuse

To ensure a consistent and unified approach to AI innovation, governance and trust, EXIM has taken steps to harmonize AI requirements across the agency:

- **Documentation of Best Practices:** Document and share best practices regarding AI governance, innovation, and risk management to ensure they are consistently applied.
- **Interagency Coordination:** Engaging in interagency coordination efforts to align our AI strategies and policies with other federal agencies, promoting a coherent and collaborative approach to AI use.
- **Continuous Improvement:** We continuously update our AI practices and policies to reflect emerging trends, technological advancements, and evolving regulatory requirements.

EXIM recognizes the importance of collaboration and knowledge sharing in advancing AI innovation.   EXIM's current technology footprint is almost exclusively based on commercial software products with little to any modifications for EXIM. In the few places that EXIM is responsible for software development, the systems are primarily transaction processing in nature and do not currently rely on AI capabilities.

To the extent EXIM were to enter this space, our efforts in this would include:

- **Custom-Developed AI Code:** Ensuring that custom-developed AI code, including models and model weights, is shared consistent with M-25-21.
- **Incentivizing Sharing:** Encouraging the sharing of AI code, models, and data with the public and other agencies by providing incentives and support for such initiatives.
- **Coordination Efforts:** Coordinating with relevant offices within EXIM to facilitate sharing and collaboration, ensuring that best practices are disseminated and adopted across the organization.

AI Talent

Building and maintaining a skilled AI workforce is crucial for advancing responsible AI innovation. EXIM's initiatives in this area include:

- **Talent/Human Resource Planning:**   As part of its annual human capital process, EXIM identifies strategic trends and emerging talent/human resources required to support EXIM's strategy.   In this year's technology team planning, while no specific positions were identified exclusive to AI, several were identified that need to, as part of their natural evolution, accrue AI skills.
- **Internal Training Programs:** EXIM's AI governance body is curating and promoting training programs to enhance AI skills within our existing workforce. These programs cover various topics, from basic AI literacy to advanced cyber and generative AI topics.

The Chief Human Capital Officer is part of EXIM's AI governance body. As mentioned, AI talent capabilities are accreting into talent search in the IT space and other job categories where AI skills are considered important for remaining up to date in information technology.

EXIM does not currently have an explicit strategy for recruiting individual AI talent. However, it will identify specific duties within position descriptions that are important for EXIM's acceleration of AI use. EXIM's partnership with its Human Capital team is essential to updating position descriptions and creating related internal training opportunities or creating new positions and developing a targeted recruitment strategy for attracting top talent for these positions.

The training and outreach activities at EXIM are well underway. Members of our governance body, focusing on this work stream, have assembled open source and other government-sponsored material available to staff. EXIM has extensively leveraged the capabilities of larger federal agencies, the Chief Artificial Intelligence Officer's Council (CAIOC), and user groups. One of the training paths is role-based (e.g., focusing on leadership, acquisition workforce, hiring teams, software engineers, administrative personnel, or others).

IMPROVING AI GOVERNANCE

AI Governance Board

Establishing an AI governance body within EXIM is a critical component of our commitment to ensuring AI technologies' responsible use. This body is designed to oversee the implementation and operation of AI systems and ensure compliance with relevant laws, regulations, and internal policies.

The AI governance body at EXIM is comprised of representatives from key offices, ensuring a comprehensive and multidisciplinary approach to AI oversight. Leadership within EXIM on the governance body includes:

- Office of the Chief Information Officer (CIO and CISO)
- Office of Communications
- Office of General Counsel
- Office of the Chief Management Officer (CMO)
- Office of the Chief Risk Officer (CRO)
- Office of the Chief Financial Officer (CFO)
- Chief Banking Officer (CBO)
- Chief Human Capital Officer (CHCO)
- Office of Contracting Services (Chief Acquisition Officer)
- Insights and Data Solutions Division (Chief Data Officer)
- Office of Ethics and Compliance (Chief Ethics Officer/Chief Compliance Officer)
- Office of External Engagement
- Office of Congressional and Intergovernmental Affairs
- Division of Research and Information Services

The AI governance body aims to achieve the following outcomes:

- **Risk Mitigation:** Identify and mitigate potential risks associated with AI, including poor operator or user practices, biases and other harms.
- **Transparency and Accountability:** Maintain transparency in AI operations and hold stakeholders accountable for their roles in AI governance.

- **Continuous Improvement:** Foster a culture of constant improvement in AI governance practices, keeping pace with technological advancements and emerging best practices.

The AI governance body will consult with external experts as appropriate and consistent with applicable laws to enhance the robustness of our AI governance framework. These consultations may include:

- **Interagency Collaboration:** Coordinating with other federal agencies to share knowledge and align best practices for AI governance.
- **Academic Institutions:** Collaborating with researchers and experts from universities and research institutions.
- **Industry Leaders:** Engaging with industry experts to gain insights into cutting-edge AI technologies and practices.

The AI governance body operates under a defined framework that includes regular meetings, a structured review process for AI projects, and transparent reporting lines to senior leadership. Key activities include:

- **Review and Approval:** Evaluating AI projects and use cases to ensure they meet legal and policy requirements before deployment.
- **Monitoring and Oversight:** Continuously monitoring AI systems for compliance and performance, with mechanisms in place for regular reviews and audits.
- **Policy Development:** Developing and updating internal AI principles, guidelines, and policies to reflect the evolving AI landscape and regulatory requirements.
- **Stakeholder Engagement:** Ensuring active engagement with internal and external stakeholders to foster a collaborative approach to AI governance.

EXIM leverages the resources, controls, and governance capabilities of the Office of Chief Information Officer which includes the Chief Information Security Officer to ensure rigor around the operationalization of AI governance and compliance.   This includes responsibility for the technology elements of the agency strategic plan, the technology Capital Planning and Investment Control (CPIC) process and various project governance and agency System Development Life Cycle (SDLC) policies where EXIM ensures various compliance requirements are brought to bear on agency technology.

Agency Policies

The agency cyber security program is routinely revised to incorporate the latest National Institute of Standards and Technology (NIST) controls including new control sets related to AI. The AI initiative’s operationalization is further augmented by the agency’s AI policy which fills policy and procedure gaps not addressed by modifications to existing policies.

As part of its fiscal 2024 and 2025 policy and procedures review, updates have already been made to existing policies to establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk. This includes updates to our Security Awareness Training program, CPIC and SDLC policies and processes. In addition, our IT Rules of Behavior and our Annual Security Awareness Training and outreach have been updated to clarify expectations for staff interaction with open-source and licensed Generative AI capabilities which are readily accessible through the agency network and personal computing environment.

AI Use Case Inventory

The creation and maintenance of AI use case inventories are essential to ensuring that EXIM comprehensively understands how AI technologies are utilized across the agency. This inventory process allows EXIM to manage AI deployments effectively, ensuring alignment with our mission and regulatory requirements.

EXIM is a small agency with no sub-agencies, bureaus, or independent components. EXIM has developed an AI policy and procedure and updated other key agency IT policies to:

- Ensure a clear understanding of what constitutes AI and a Use Case
- Develop a clear internal policy and process for periodically surveying the organization for AI use cases and routine review of use cases that aligns with requirements.
- Establish responsibility for submission and publication of use cases.
- Identify use cases that require special attention (e.g., rights and benefits impacting).
- Ensure previously excluded use cases are revisited periodically, as appropriate, for later inclusion.
- Formalize a process of issuing, denying, revoking, and tracking use cases and certifying waivers.

Due to EXIM's small size and current posture regarding AI, EXIM is leveraging robust, well-established technology review processes within the Office of the Chief Information Officer that reviews the introduction of any new technology at EXIM and periodically review all existing IT investments. When these activities detect any existing or planned introduction of AI, they engage our AI governance body for appropriate follow-up.

To ensure that our AI use case inventory is comprehensive and complete, EXIM further employs:

- **Education**: EXIM, through its AI governance body, has prepared basic education of the compliance requirements for AI that are now integrated into all staff members onboarding and annual recurring Security Awareness Training. AI governance body members are further informed about more specific policies and procedures.

- **Stakeholder Engagement:** Engaging with key stakeholders, including Chief Data Officers, Chief Information Officers, Chief Technology Officers, and program managers to identify AI use cases.
- **Cross-functional Collaboration:** Collaborating across various departments ensures that all potential AI applications are captured and evaluated.
- **Documentation and Tracking:** Maintain detailed documentation and track all AI use cases to ensure they are accurately represented in the inventory.

While EXIM aims to maintain a transparent inventory of AI use cases, certain use cases may be excluded based on specific criteria:

- **Mission Risk:** Use cases that, if disclosed, could negatively impact, or create risks to the agency's mission, employees, customers, or the public.
- **Confidentiality Agreements:** Use cases subject to confidentiality agreements with other agencies, customers, employees, or stakeholders.
- **Security Concerns:** Use cases that involve sensitive or classified information that cannot be publicly disclosed.

EXIM is committed to periodically revisiting and validating AI use cases in its inventory to ensure accuracy and relevance. This process includes:

- **Periodic Reviews:** Conducting no less than annual reviews of the AI use case inventory to identify any changes or updates needed.
- **Validation Criteria:** Predefined criteria are used to reassess use cases and determine whether previously excluded cases should be included or whether any new cases meet the exclusion criteria.
- **Approval and Oversight:** The Chief AI Officer (CAIO) and the AI governance body is engaged in the review and validation process to ensure accountability and transparency.

In line with our commitment to transparency, EXIM makes AI use case inventories, according to the reporting guidance, publicly available on its website. The inventory is updated no less than annually to reflect new AI use cases and any changes to existing ones. EXIM's public inventory includes:

- **Descriptions of AI Use Cases:** Provide clear and concise explanations of each AI use case, including its purpose, scope, and expected outcomes.
- **Compliance Information:** Provide designated compliance information per M-25-21 and any other subsequent standards.

The main clearinghouse for documenting and sharing best practices is the AI governance body and its members who participate, not only in sharing CAIOC community information, but also are participating in communities of interest for their discipline.

The agency CIO and CISO are members of the small agency CIO and CISO council, Privacy Council, and members of DHS/CISA communities. The CIO, CISO and CTO also participate in non-government sponsored communities of interest which have vibrant AI-focused best practices sharing.

Other key EXIM officials, the Chief Management Office, Chief Acquisition Officer, Chief Risk Office, Chief Financial Officer, and Chief Human Capital Officer are members of federal user groups and private sector organizations that, like the technology community, share developing AI best practices, risks and innovation through the lens of their function and professional area of responsibility.

FOSTERING PUBLIC TRUST IN FEDERAL USE OF AI

Determinations of Presumed High-Impact AI

To ensure the responsible deployment of AI, EXIM has established a process for determining which AI use cases are considered safety-impacting or rights-impacting:

- **Review Process:** Each current and planned AI use case undergoes a review to assess whether it matches the definitions of safety-impacting or rights-impacting AI defined in Section 5 of OMB Memorandum M-25-21.
- **Criteria for Assessment:** Our assessment criteria include the potential for physical harm, the impact rights or benefits, and the degree of automation in decision-making processes.
- **Supplementary Criteria:** EXIM may develop additional criteria tailored to our specific operations to guide safety and rights-impacting AI decisions.

As described above, the agency AI governance body is tasked with ensuring the proper development and implementation of use case identification and review which also includes rights and safety impacting scenarios. The AI policy and related procedures ensure a comprehensive review by agency stakeholders.

Currently, the Agency has no AI use cases in the category of Rights or Safety impacting and the agency, therefore, has not created any additional criteria for the identification of rights or safety impacting or criteria to guide waiver decisions.

EXIM's AI policy and its sections related to use case identification and inventorying will be where EXIM will formalize the process of issuing, denying, revoking, and tracking safety-impacting or rights-impacting AI and certifying waivers as appropriate.

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

Implementing effective risk management practices is essential to mitigate the risks associated with AI. Our agency AI policy ensures:

- **Comprehensive Risk Assessments:** Conduct comprehensive risk assessments for all AI applications, identifying potential hazards, vulnerabilities, and impact on stakeholders.
- **Minimum Risk Management Practices:** Document and validate the implementation of minimum risk management practices, including data privacy, security measures, and contractual considerations.
- **Risk Management Framework:** Develop and maintain a risk management framework that outlines the procedures for identifying, assessing, mitigating, and monitoring risks throughout the AI lifecycle.

The agency has updated its SDLC policy, its CPIC process and issued guidance to agency staff regarding the contents of M-25-21 and the importance of clauses in M-25-21 regarding its obligations to protect the agency from non-compliant safety-impacting or rights-impacting AI from being deployed to the public.

EXIM's AI governance body includes representatives from the Office of Contracting Services who have a working understanding of M-25-21 as well as close working relationship with the CIO and CISO on compliance with various technical mandates regarding the procurement of technology for the agency.

Outreach and training to the general staff of the agency sponsored by the AI governance body includes key compliance elements related to M-25-21 as well as other federal mandates regarding the use of AI.

In certain circumstances, it may be necessary to issue waivers for one or more of the minimum risk management practices. EXIM, as part of its AI policy, has outlined a straightforward process for this:

- **Criteria for Waivers:** Develop criteria to guide the decision to waive risk management practices, ensuring that waivers are granted only when necessary and justified.
- **Issuance and Revocation:** Establish procedures for issuing, denying, revoking, tracking, and certifying waivers, with oversight from the Chief AI Officer (CAIO) and the AI governance body.
- **Documentation and Transparency:** Maintain detailed records of all waiver decisions to ensure transparency and accountability.

As of the date of this report, EXIM has no AI use cases requiring a waiver.   As part of our normal policy review process, our AI policy and associated risk management practices will be updated as we develop maturity in this space.

APPENDIX A: TERMS AND DEFINITIONS

Artificial Intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis, and use model inference to formulate options for information or action.

Chief AI Officer (CAIO): A senior executive responsible for overseeing the agency's development and implementation of AI strategies, policies, and governance. The CAIO ensures compliance with standards and regulatory requirements and coordinates AI initiatives across the organization.

Chief AI Officer Council (CAIOC): An interagency group led by OMB and comprised of Agency CAIOs to support the roll-out of M-25-21 and share best practices for the implementation of AI strategies, policies, and governance. The CAIOC also assists in coordinating AI initiatives across the Federal Government.

AI Governance is the framework, processes, and policies implemented to ensure the ethical, legal, and responsible use of AI within an organization. It includes establishing governance bodies, principles, and guidelines to oversee AI applications.

AI Governance Body: A multidisciplinary committee comprising representatives from key offices within the agency. This committee is responsible for overseeing the implementation and operation of AI systems. The governance body ensures that AI initiatives align with standards, regulatory requirements, and the agency's strategic goals.

AI Use Case Inventory: A comprehensive list of all AI applications and use cases within an organization, detailing their purpose, scope, and compliance with regulatory standards. The inventory is used to manage AI deployments effectively and ensure transparency.

Safety-Impacting AI: AI applications that have the potential to cause physical harm or pose significant safety risks. These use cases require rigorous risk assessments and compliance with stringent safety standards.

Rights-Impacting AI: AI applications that can potentially affect individuals' civil rights, privacy, or other fundamental rights. These use cases require careful consideration of their implications and compliance with legal and regulatory requirements.

Generative AI: A class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content, such as images, videos, audio, text, and other digital content.

Risk Management Framework: A structured approach for identifying, assessing, mitigating, and monitoring risks associated with AI applications. The framework includes preventive controls, monitoring mechanisms, and procedures for managing incidents and non-compliance.

Transparency and Accountability: Principles ensuring that the development and deployment of AI systems are open and transparent, with clear documentation and oversight to hold stakeholders accountable for their roles in AI governance.

Responsible AI Use: The capabilities to innovate and promote the responsible adoption, use, and continued development of AI, while ensuring appropriate safeguards are in place to protect privacy, civil rights, and civil liberties, and to mitigate any unlawful discrimination, consistent with the AI in Government Act.

AI Talent Development: Initiatives and programs that aim to build and maintain a skilled AI workforce through targeted recruitment, training, and career development opportunities.

Technology Review Process: A formal procedure for evaluating technology requests, including AI applications, to ensure they meet technical, ethical, and regulatory standards before approval and implementation.