U.S. Trade and Development Agency (USTDA) AI Compliance Plan for OMB Memorandum M-25-21 – September 2025

Issued by Samuel Kwon, USTDA General Counsel

Pursuant to the AI in Government Act of 2020, the Advancing American AI Act of 2022, Executive Order 14179, and Office of Management and Budget ("OMB") Memoranda M-25-21, (*Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*) and M-25-22 (*Driving Efficient Acquisition of Artificial Intelligence in Government*), USTDA hereby adopts the following Compliance Plan for Artificial Intelligence ("AI"):

1. Driving AI Innovation

Removing Barriers to the Responsible Use of AI

- In April 2024, USTDA designated the Director of Management Operations position[1] to also serve as the Agency's Chief AI Officer ("CAIO").
- As a small agency, USTDA has limited funding and staffing resources to effectively pursue AI use cases and instead leans upon the lessons learned and best practices of the interagency.
- USTDA will consider possible future AI use case scenarios and formulate budgetary requests, as appropriate, to garner the resources necessary to effectively and responsibly implement AI use cases in alignment with M-25-21 and M-25-22.

Sharing and Reuse

- USTDA does not intend to develop AI code – including models and model weights for AI applications.
- USTDA's CAIO and Office of the Chief Information Officer ("OCIO") will continue to engage in the broader interagency discussions as AI use cases evolve across the federal government, including via the CAIO Council and the Small Agency Committee.

AI Talent

- As a small agency, USTDA does not have any standalone staffing resources dedicated to AI work and instead relies upon a small OCIO team who cover a broad range of IT related activities and projects.
- USTDA will continue to leverage OPM's Gov2Gov educational series and other shared service training and information sharing opportunities to continue to develop and inform AI knowledge across the Agency.
- The CAIO will continue to share resources on AI best practices within the Agency via internal email distribution and on the Agency's internal AI Information Page.
- USTDA will also coordinate with AI innovators and experts across academia, non-governmental organizations, and the private sector to identify and deploy potential trainings for staff on the capabilities, limitations, and risks associated with AI.

[1] USTDA's Director of Management Operations position is currently vacant. Until that position is staffed, the role of CAIO will be handled by the agency's Chief Information Officer. When the Director of Management Operations role is filled, USTDA will notify OMB and update this information at ustda.gov/ai in compliance with M-25-21.

2. Improving AI Governance

AI Governance Board

- USTDA has adopted an "AI Acquisition Policy" (attached and incorporated herein as Annex A), which establishes the framework and procedures for acquiring AI systems and services to ensure internal collaboration, compliance with federal mandates, and proactive risk management as required by M-25-21 and M-25-22.
- As part of the AI Acquisition Policy, USTDA has established a protocol to deploy a cross-functional team (the "AI Review Team") to ensure well-rounded decision-making, conduct risk assessments, maintain appropriate oversight, and promote appropriate escalation procedures for AI.
- USTDA will leverage the AI Review Team to review and assess any potential AI use cases and AI acquisitions and provide the appropriate governance of their implementation and use.

Agency Policies

- Aside from this AI Compliance Plan and the incorporated AI Acquisition Policy, USTDA is in the process of creating a Generative AI Policy. These policies will together establish the appropriate safeguards and oversight of AI procurements and staff's use of generative AI, for example by subjecting each proposed use case to review by a cross-functional team. USTDA will ensure any AI policies that are drafted in the future are consistent with M-25-21 and M-25-22.

AI Use Case Inventory

- In August 2024, USTDA's OCIO conducted a comprehensive review of the Agency's deployed infrastructure, software, and applications and identified that three (3) AI products are in active use as part of the Continuous Diagnostic and Mitigation Program cybersecurity package provided to USTDA by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency ("DHS/CISA"). Additionally, in May 2024 USTDA retained the services of a due diligence vendor that utilizes AI as part of its research services to review and consolidate publicly available information on searched subjects for evaluation, refinement, and analysis by the vendor's staff. All four of these AI products are commercial-off-the-shelf and have not been modified.
- USTDA provided a complete AI use case inventory to OMB and publicly posted the inventory to ustda.gov/ai in December 2024.
- On an annual basis, the CAIO will conduct a reassessment of the Agency's enterprise-wide environment for active AI use cases in compliance with M-25-21.
- Should a future assessment of the enterprise-wide environment identify any new AI use cases, then the AI Review Team would review those use cases and determine if they are excluded or not subject to inventory based upon guidance in M-25-21.

3. Fostering Public Trust in Federal Use of AI

Determinations of Presumed High-Impact AI

- In consultation with USTDA's OCIO and Office of General Counsel, the Agency's CAIO determined that USTDA does not currently utilize, nor does the Agency intend to utilize,

any high-impact AI as defined in M-25-21.

- USTDA will utilize its AI Acquisition Policy and AI Review Team to review and assess the possibility of high-impact as defined in M-25-21 for any potential AI use cases and provide the appropriate governance for their implementation and use or denial of use as appropriate.
- USTDA will continue to leverage the best practices of the interagency as well as guidance from OMB and DHS/CISA.

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

- USTDA's Cybersecurity & Privacy Program Risk Management Plan ("RMP") and the AI Acquisition Policy together document the agency's minimum risk management practices, with the latter specific to AI. The Agency will utilize the annual FISMA audit, assessment and authorization process to validate their implementation.
- USTDA will follow its RMP and the AI Acquisition Policy and will utilize the AI Review Team to prevent non-compliant high-impact AI from being deployed to the public.
- By following the RMP and AI Acquisition Policy and utilizing the AI Review Team, USTDA will ensure that any non-compliant AI being utilized by the agency or its staff is terminated in a swift and appropriate manner.

ANNEX A

USTDA AI Acquisition Policy

1. Purpose

This policy, the "USTDA AI Acquisition Policy", is a crucial document establishing a framework and procedures for acquiring Artificial Intelligence (AI) systems and services within our agency. This policy ensures internal collaboration, compliance with federal mandates, and proactive risk management as required by OMB Memoranda M-25-21 and M-25-22.

2. Scope

This policy, which applies to all U.S. Trade and Development Agency (USTDA) AI systems and services acquisitions, regardless of scale, complexity, or intended use, is comprehensive in its coverage. It encompasses all AI technologies, including but not limited to machine learning (ML), generative AI (GenAI), natural language processing (NLP), computer vision, and any AI system that may impact rights, safety, privacy, or agency operations. The policy covers the entire lifecycle of AI procurement, from initial planning and risk assessment through acquisition, deployment, monitoring, and eventual decommissioning. This policy applies to new acquisitions and modifications to existing AI systems, ensuring that all AI solutions procured or used by the agency meet ethical, legal, and performance standards in compliance with OMB Memoranda M-24-21 and M-24-22, as well as related federal guidelines.

3. Roles and Responsibilities

Several USTDA resources are key to the implementation of this AI acquisition policy:

- **Chief Information Officer (CIO):** Oversees AI acquisition security and risk management.
- **Chief AI Officer (CAIO):** Ensures AI acquisitions comply with ethical standards and federal regulations.
- **Acquisition Management Team (AQM):** Coordinates procurement activities and ensures compliance with acquisition procedures.
- **Office of General Counsel (OGC):** Reviews AI provider Terms of Service (ToS) and End-User License Agreements (EULAs); provides legal and ethics guidance on AI acquisitions and use.
- **Senior Agency Official for Privacy (SAOP):** Ensures compliance with privacy laws, especially regarding Personally Identifiable Information (PII).
- **Director of Management Operations (DMO):** Oversees AI project implementation, ensuring alignment with agency goals and proper risk management.
- **Cross-Functional Review Team:** This team includes all of the above USTDA departments, which are comprised of personnel specializing in IT (including the CIO), cybersecurity, privacy, ethics, legal, and budgeting, to support AI acquisition decisions and risk assessments.

4. Policy Requirements

4.1. Internal Agency Collaboration

Policy Development: USTDA shall ensure cross-functional collaboration before initiating any AI acquisition.

Compliance Assurance: All acquisitions must ensure compliance with OMB M-24-21, M-24-22, and USTDA's AI Compliance Plan, of which this USTDA AI Acquisition Policy is a part.

4.2. Acquisition Planning and Review

- Initial Review:
  - Planned AI acquisitions must undergo an initial review by relevant agency officials.
  - The review determines whether additional AI performance and risk management practices (per M-24-21) are necessary.
- Review Checklist Includes:
  - Intended use and scope
  - Risk assessment (including rights and safety impacts)
  - Potential for adverse decisions
  - Vendor's AI risk management practices
  - Data privacy assessment
  - Vendor flexibility/lock-in assessment
- Escalation Protocol:
  - Escalate complex acquisitions or those with significant risk (including risks identified during acquisition, implementation, monitoring, or decommissioning) to Senior USTDA Leadership.

4.3. Cross-Functional Collaboration

USTDA shall foster collaboration among key stakeholders from multiple disciplines to ensure well-rounded decision-making. This includes officials in:

- **AQM:** To ensure procurement complies with federal acquisition regulations and promotes competitive sourcing.
- **IT and Cybersecurity:** To assess technical feasibility, integration capabilities, and security risks.
- **Privacy and Ethics:** To evaluate potential impacts on individual rights, data privacy, and equity.
- **OGC:** To review legal implications, ToS, and EULAs.
- **Finance:** To ensure financial accountability and cost-effectiveness.
- **Data Management and Program Evaluation:** To validate data quality, source appropriateness, and methods for evaluating AI performance and outcomes.

4.4. Risk Management and Compliance

Risk Assessments: All AI acquisitions must undergo a risk assessment covering:

- Bias and fairness:
  - Transparency and explainability

    - Privacy and security risks
    - Rights and safety impacts assessments
- Degradation monitoring:
    - Vendors must implement performance monitoring and submit annual reports on system behavior and potential degradation.
- Incident reporting:
    - Vendors and USTDA personnel must report AI incidents to the CIO and CAIO within 24 hours of discovery.

4.5. Post-Acquisition Oversight

- **Annual Reviews:** USTDA shall conduct annual software/service evaluations to assess AI system performance, risk mitigation measures, and compliance with agency goals.
- **Annual Reports:** Contractors must submit yearly reports to USTDA detailing AI system functionality, training data sources, and any significant modifications.

5. Vendor and Contractual Obligations

- **Vendor Due Diligence:** Vendors must demonstrate adherence to responsible AI practices and provide comprehensive documentation to USTDA on AI training, testing, and validation data.
- **Mandatory Contract Clauses:** When acquiring AI systems and services, USTDA shall include contract clauses specific to ensuring vendor accountability for system performance, risk management, and compliance. In the event USTDA seeks to acquire high-impact AI, USTDA shall include additional contract clauses specific to that acquisition.

6. Monitoring, Evaluation, and Reporting

To ensure the responsible and effective use of AI systems, USTDA shall establish comprehensive monitoring, evaluation, and reporting mechanisms that cover the entire AI lifecycle – from acquisition to deployment and eventual decommissioning. These processes are critical for managing risks, ensuring compliance, and promoting transparency in AI use.

- **Performance Monitoring:** USTDA shall implement continuous monitoring processes to assess AI system performance against predefined metrics. This includes evaluating accuracy, reliability, efficiency, and tracking real-world outcomes. Monitoring should also identify and address system degradation, unintended behavior, and biased outputs.
- **Degradation Monitoring:** Regular assessments must be conducted to detect any performance degradation or changes in system behavior over time. This includes monitoring for issues affecting rights, safety, or system integrity. Contractors are required to submit Degradation Monitoring Reports to USTDA every year, documenting performance trends and any remedial actions taken.
- **Unwanted System Behavior:** USTDA shall monitor and work with vendors to mitigate unwanted system behaviors, such as generating harmful, biased, or erroneous outputs. This includes setting up alerts and triggers for abnormal system activities and establishing protocols to retrain or adjust AI models as necessary.
- **Risk Monitoring for Rights and Safety:** USTDA shall give special attention to high-impact AI systems. In particular, USTDA shall (i) ensure that vendors establish continuous

monitoring (ii) evaluate whether these systems pose risks to civil rights, privacy, or public safety and (iii) determine whether additional safeguards are required.

7. Escalation Procedures

Certain conditions related to AI acquisitions or AI performance must be escalated to USTDA's senior leadership. This includes, but is not limited to:

- Escalation Triggers:
  - AI acquisitions or AI performance issues that:
    - Pose high risks to civil rights or safety.
    - Involve high-impact AI (as defined in M-24-21).
    - Involve sensitive data or critical infrastructure.
    - Have significant budgetary impacts.
  - Situations where consensus among stakeholders cannot be reached.
- Escalation Path:
  - Contracting Officer and/or CAIO → Senior USTDA Leadership.

8. Training and Awareness

All personnel involved in AI acquisition and management must undergo mandatory training on the following:

- AI ethics and bias
- AI risk management
- Privacy and security in AI systems

9. Document Control and Revisions

This USTDA AI Acquisition Policy will be reviewed and updated annually or as required based on federal regulations or USTDA practice changes.

10. Effective Date

This USTDA AI Acquisition Policy shall be integrated into USTDA's existing AI Compliance Plan and is effective upon issuance. It will remain in effect until further notice.