Department of State
Compliance Plan for OMB Memorandum M-24-10 – September 2024

Prepared by: Dr. Matthew Graviss, Chief Data and Artificial Intelligence Officer

Publication Date: September 23, 2024

TABLE OF CONTENTS

DEPARTMENT OF STATE COMPLIANCE PLAN FOR OMB MEMORANDUM M-24-10 – SEPTEMBER 2024……1

1. STRENGTHENING AI GOVERNANCE ……3

Overview ……3

AI Governance Bodies ……3

AI Use Case Inventories ……4

Reporting on AI Use Cases Not Subject to Inventory ……4

2. ADVANCING RESPONSIBLE AI INNOVATION……5

AI Strategy ……5

Removing Barriers to the Responsible Use of AI ……5

AI Talent ……6

AI Sharing and Collaboration ……8

Harmonization of Artificial Intelligence Requirements ……9

3. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE ……9

Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting ……9

Implementation of Risk Management Practices and Termination of Non-Compliant AI……10

Minimum Risk Management Practices ……11

APPENDIX A: AI GOVERNANCE BODIES ……14

Enterprise Governance Board (EGB): ……14

AI Steering Committee (AISC): ……14

1. STRENGTHENING AI GOVERNANCE

Overview

The Department of State has strengthened its AI governance bodies, and democratized access to AI policy, guidance, and resources. In 2024, the Department launched the AI State Hub, a resource and "one-stop shop" for all things AI. The platform is accessible to all Department personnel with the most up to date information on safe, secure, and trustworthy AI use. This includes 20 FAM 201 AI Policies and Procedures, AI procurement best practices, and guidance for using publicly available generative AI (GenAI) services.

AI Governance Bodies

The Department of State implements AI governance at the executive, strategic, tactical, and operational levels (see **Appendix A** for membership lists). At the executive level, the **Enterprise Governance Board (EGB)** serves as the Department's AI Governance Board. The EGB is a forum for senior Department leaders to discuss strategic issues and provide input into enterprise-level decisions on a regular basis. Its purpose is to enhance transparency, agility, and alignment of resources with priorities, and to increase the speed of enterprise-level decision-making. The Deputy Secretary for Management and Resources (D-MR) chairs the EGB and the Chief Data and AI Officer (CDAO) vice-chairs during AI Governance Board sessions.

The **Enterprise Data and AI Council (EDAC)** provides strategic governance. The EDAC centrally promulgates and coordinates policy and standards for AI governance in the Department. It is accountable for implementing the Enterprise Data Strategy (EDS) and Enterprise AI Strategy (EAIS). The EDAC is chaired by the CDAO and comprised of Principal Deputy Assistant Secretaries and Deputy Assistant Secretaries from across the Department, as well as the Statistical Official and the Department's Evaluation Officer(s).

In 2024, the Department established the **AI Steering Committee (AISC)** to provide tactical governance and advise the EGB, CDAO, and the Chief Information Officer (CIO) on applied AI. The AISC is co-chaired by the Responsible AI Official (RAIO) and the Enterprise Chief Information Security Officer (E-CISO). The AISC facilitates enterprise-wide AI collaboration on applied AI policy, guidance, and communications through the **AI Communications and Training Working**

Group and topical policy Working Groups, as needed. The AISC reports to the EDAC and CDAO on the Department's implementation of the EAIS, advising on AI technologies, compliance, and collaboration. The AISC also promotes responsible AI use, identifies risks, enacts necessary policies and guidelines, and monitor AI initiatives across the Department.

At the operational level, 20 FAM 201.1-3(F) articulates additional governance requirements to ensure the Department's **AI Use Case owners** comply with Department and federal policy. 20 FAM 201 is regularly updated with guidance for AI Use Case owners as federal requirements evolve.

Members of the Department's governance bodies consult with external experts on a case-by-case basis including the National Institute of Standards and Technology (NIST), the Chief AI Officers Council (CAIOC), and the AI Safety Institute (AISI).

On behalf of the Under Secretary for Management (M), the Center for Analytics in the Office of Management Strategy and Solutions (M/SS/CfA), managed by the CDAO, acts as a central hub for all things applied data and Artificial Intelligence (AI) within the Department of State (DOS).

AI Use Case Inventories

M/SS/CfA manages an annual data call to complete the AI Use Case Inventory according to OMB requirements. The CDAO validates and verifies each entry with the AI Use Case Owner, shares the draft AI Use Case Inventory with Department leadership for clearance, and posts the final public inventory on state.gov/artificial-intelligence/.

To ensure comprehensiveness and completeness, the M/SS/CfA leads discussions in the AISC and other AI governance bodies about the AI Use Case Inventory process. The M/SS/CfA also holds open information sessions, general office hours for all Department staff, targeted office hours for existing AI Use Case owners and data scientists and socializes these engagements and policy on AI.State, an internal SharePoint site available to all employees.

Reporting on AI Use Cases Not Subject to Inventory

While certain AI Use Cases are exempt from reporting, the Department nonetheless collects information on these use cases during its annual AI Use Case Inventory data call per 20 FAM 201.1-3(E). AI Use Case owners with AI Use Cases that meet the criteria are informed about the

individual reporting exemption and the need only to report aggregate metrics during the stakeholder engagement phase. During the leadership reviews, the Department validates the determination for excluding an AI Use Case from public disclosure and individual inventory**.** AI Use Cases are reviewed on an annual basis, per 20 FAM 201.1-3(E). The criteria used for individual inventory is that laid out by 44 U.S.C. 3552(b)(6) and 20 FAM 201.

1. ADVANCING RESPONSIBLE AI INNOVATION

AI Strategy

The Department released its first-ever AI strategy, the Enterprise AI Strategy (EAIS) in October 2023 to help unify the Department around a singular vision: "The Department of State will responsibly and securely harness the full capabilities of trustworthy artificial intelligence to advance United States diplomacy and shape the future of statecraft." The EAIS comprises four major strategic goals and objectives:

- Leverage secure AI infrastructure by enabling AI technology integration, fully utilizing infrastructure of AI adoption at Department scale and modernizing acquisition of AI tools.
- Foster a culture that embraces AI technology by providing AI training and support services, developing new opportunities for AI talent, and promoting responsible use of AI.
- Ensure AI is applied responsibly by establishing and maintaining AI governance and policy, brokering appropriate access to AI-ready data, and facilitating data quality assurance.
- Innovate in the AI space by identifying opportunities, facilitating responsible experimentation, and scaling successes.

Removing Barriers to the Responsible Use of AI

The Department has identified potential barriers to responsible use of AI, including barriers to responsible GenAI listed in NIST AI 600-1, such as data privacy, confabulations, harmful bias and homogenization, human-AI configuration, and others. As part of broader efforts to address the barrier of data privacy, the Department has onboarded, tested, and is maintaining a vetted GenAI model that is safe to process Sensitive but Unclassified (SBU) information for Department use. In addition, the Department leverages its AI governance bodies to establish policies and procedures

that manage the risks of confabulation, harmful bias and homogenization, and human-AI configuration. The Department, for instance, has created and maintains guidance to have a human-in-the-loop in AI implementation and oversight, for example, as outlined in 20 FAM 201 and in guidance on publicly available GenAI services. The Department stood up an independent testing, evaluation, validation, and verification (TEVV) team that focuses on measuring baselines and monitoring performance by operationalizing the risk management practices established in NIST AI Risk Management Framework.

Technically, potential barriers include access to a limited number of approved AI tools and a lack of an open-source library to share code and models among authorized development teams. To address these challenges, the Bureau of Diplomatic Technology (DT) and M/SS/CfA are expanding access to enterprise tools and planning to develop an "AI Marketplace" to allow bureaus, offices, and posts to rapidly access approved and centrally monitored AI tools. Additionally, M/SS/CfA is piloting tools to share code, datasets, and models for internal evaluation and rapid development.

The Department provides bureaus, offices, and posts with updated guidance, training materials, and support through AI.State, the Department's central information hub for AI. In 2023, the Department released 20 FAM 201 to establish guardrails for AI. In January 2024, the Department released additional internal guidance relating to publicly available GenAI tools, including permitted use cases, information security requirements, terms of service reviews, and records management policy. The Department has also created and shared guidance related to labeling, AI procurement best practices, and intellectual property rights protections. Department policy mandates that all generative AI outputs, regardless of audience or other circumstance, be reviewed by a human for accuracy and appropriateness to manage risk and ensure adequate oversight. This requirement is reinforced in 20 FAM 201, internal guidance on the use of publicly available GenAI services, topical guidance (for example, internal guidance on translation), and system-specific rules of behavior. Finally, the Department is developing additional detailed guidance and training materials on implementing risk management for rights-impacting and safety-impacting AI.

AI Talent

The Department is focused on hiring qualified candidates who have extensive knowledge of emerging technologies and an understanding of and curiosity for trends and innovation in data

science and AI. The Department has identified the need for the following specific skillsets and skill levels: Data Scientists at the GS-13 and GS-14 levels; Data Analysts at the GS-13 and GS-14 levels; and data and AI leadership at the GS-15 levels.

In December 2023, M/SS/CfA leveraged the GW-007 Direct Hire Authority to initiate a Department-wide hiring announcement for **data scientists with an AI tag**. M/SS/CfA is certifying 1560 and 0343 standard position descriptions (SPDs) (each at the GS-13 and -14 levels) with AI responsibilities to leverage GW-007 and GW-009 respectively in support of E.O. 14110. A new list of applications for GS-13 data scientists, including those with AI skillsets, for September 2024 is in progress by the Bureau of Global Talent Management (GTM), following the expiration of the previous list on August 7, 2024, using GW-007.

The Department continues to recruit and hire AI personnel with an understanding of AI techniques, technologies, principles, and ethics through the **Bureau Chief Data Officer (BCDO) program** and **locally employed data scientist hiring**. Consistent with the requirements in Section 6302(d) of the Department of State Authorization Act of 2023 (Div. F, P.L. 118-31), M/SS/CfA created the BCDO position to lead data and AI efforts in regional and functional bureaus by, in part, strengthening capacity, coordinating AI efforts, and cultivating data culture within their bureau. The Department is expanding these capabilities due to the initial impact of the first BCDOs. As of September 1, 2024, 15 BCDOs have joined the Department. As a part of Secretary Blinken's Modernization Agenda, M/SS/CfA, in collaboration with GTM's Office of Overseas Employment (GTM/OE), also introduced a new LE Staff Data Scientist SPD, to attract talented personnel that can enhance data-informed decision making, operational efficiencies, and innovation at consulates and embassies. To maintain a diverse pipeline of AI talent, the Department attends career fairs to recruit candidates and connect with students to provide information about the Department's data and AI opportunities.

In addition to hiring AI talent, the Department's AI training efforts upskill AI-adjacent roles, such as program managers, and the broader Department workforce. The Department centralizes training opportunities through the AI.State SharePoint site to empower its workforce with AI training. In close coordination with the Foreign Service Institute, the Department created a new AI-specific course offering as part of the School of Applied Information Technology (SAIT)'s New Technology Seminars, **PS 322: Introduction to Artificial Intelligence and ChatGPT**. Similarly, the Department is developing a new GenAI workshop titled, **"Practical Application of AI in the**

Department," set to launch in October 2024. The topic of AI is likewise integrated in annual mandatory trainings, such as the Annual Mandatory Counterintelligence and Insider Threat Awareness Training courses, and regularly scheduled tradecraft courses to help orient new hires to the Department's AI policies, resources, and tools. **AI.State** also facilitates independent learning through a centralized use case repository (searchable by role and topic), links to internal learning webinars, self-paced training videos for common use cases, AI research and reporting, and a compendium of publicly available commercial resources on AI. Promoting ready access to a variety of materials allows Department employees to tailor AI training opportunities to their specific needs and roles.

The Department convenes an AI Innovator Community of Practice to share AI resources, use cases, best practices, and specific impact metrics to accompany AI technologies that will establish parameters for the expected benefits of use.

AI Sharing and Collaboration

The Department of State is developing a plan to ensure that custom-developed AI code, including models and model weights, is shared consistent with Section 4(d) of M-24-10 by adhering to the following process. This includes updates to AI governance bodies and Department policies as necessary. Key considerations include:

1. **Compliance with Data Handling Policies:** All AI code and models must be handled in accordance with the Department's data policies, ensuring that SBU data processed and shared in a manner consistent with 12 FAM 540.
2. **Access Control:** Access to AI code and models will be restricted to authorized Department personnel who have been cleared to handle SBU data. This includes ensuring that only users with State.gov or Fan.gov accounts can access the systems where the AI code is stored.
3. **Documentation and Transparency:** Detailed documentation will be required for all custom-developed AI code, including the models and model weights. This documentation will include information on the development process, data sources, and any modifications made to the models.

4. **Review and Approval:** Before any AI code or models are shared outside of the original development team, they will undergo a thorough review and approval process to ensure compliance with Section 4(d) of M-24-10. This includes verifying that the code does not contain any classified information and that it adheres to the Department's ethical and diversity standards.
5. **Feedback and Reporting:** Users are encouraged to provide feedback and report any issues or bugs through the specific application. This feedback is used to continuously improve the AI models and ensure they meet the required standards.
6. **Training and Support:** AI Use Case owners will be required to provide training opportunities and support for users to ensure they understand how to use the specific AI tools responsibly.

Due to the sensitivity of AI-related data and code, the Department does not make all datasets widely available to external audiences. Internal audits and reviews will be conducted by the RAIO and/or bureau-specific independent reviewers of AI-related data and code. The M/SS/CfA has designed processes to share code, datasets, and models for internal evaluation. Currently, the process is in a pilot phase with select projects and will be evaluated for limited public disclosures.

Harmonization of Artificial Intelligence Requirements

The Department harmonizes AI requirements and best practices through AI.State, accessible to all Department employees. Ensuring the Department's employees have ready access to these resources promotes responsible innovation while enabling oversight and governance. M/SS/CfA maintains AI.State, which compiles key AI resources on policy, learning, and available products and tools. AI.State curates best practices in AI governance, innovation, and risk management from key offices and bureaus, such as M/SS and DT, as well as users across the Department. Department personnel may submit tools, best practices, events, recommend trainings, and AI use cases, further advancing knowledge sharing across the agency.

2. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights Impacting

The Department reviews AI Use Cases during the annual AI Use Case Inventory, both to verify if the AI Use Case is rights-impacting and/or safety-impacting and to check for compliance with minimum risk management practices. The Department is developing internal guidance on obtaining appropriate approvals for use and risk management for rights-impacting and safety-impacting AI. This guidance and any supplemental criteria will be published in the Foreign Affairs Manual (FAM) following consultation and clearance with AI governance bodies. The Department is following the OMB Guidance for 2024 Agency Artificial Intelligence Reporting per EO 14110 issued on August 14, 2024, and has not developed any separate criteria to guide a decision to waive one or more risk management practices for a particular AI Use Case.

The Department will track requested waivers of minimum risk management practices along with other information about each AI Use Case during the data call process of the AI Use Case Inventory. The CDAO will then review and report the details of each waiver as part of the annual AI Use Case Inventory.

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

The Department is developing internal guidance on risk management for rights-impacting and safety-impacting AI, to be published in the FAM and Foreign Affairs Handbook (FAH). This guidance will incorporate OMB M-24-10 requirements and Department risk management guidance, outlined in 2 FAM 030. To provide oversight and ensure compliance, AI Use Case owners will be required to seek approval from the Department's CDAO to use a potentially rights-impacting or safety-impacting AI Use Case. The AI Use Case Owners will be required to implement the risk management practices mandated by the Department's policy priority before and after approval. AI Use Case owners will then certify their compliance with the minimum risk management practices annually through the AI Use Case Inventory process. If the CDAO and/or AISC determines that an AI Use Case is non-compliant, the AI Use Case owner must terminate the AI Use Case and in order to restart the AI Use Case, the owner of that use case must develop a compliance plan under the supervision of M/SS/CfA.

AI Use Case owners are responsible for terminating non-compliant rights-impacting or safety-impacting AI Use Cases at the direction of the CDAO. The Department is also prioritizing enterprise AI tools to facilitate centralized oversight and governance. Any AI product must be

approved for use by M/SS/CfA and DT, and a bureau, office, or post that wants to use AI tools must first leverage enterprise offerings before purchasing new AI solutions. This allows for a streamlined process in the event an AI product falls out of compliance, at which point the Department can discontinue its approval and use of the AI product.

Minimum Risk Management Practices

The Department is developing internal guidance on risk management for rights-impacting and safety-impacting AI, to be published in the FAM and FAH. This guidance will incorporate OMB M-24-10 requirements and Department risk management guidance, outlined in 2 FAM 030. To provide oversight and ensure compliance, AI Use Case owners will be required to seek approval from the CDAO before implementing any potentially rights-impacting or safety-impacting AI Use Cases. AI Use Case Owners will be required to implement the risk management practices mandated by the Department's policy priority before and after approval. AI Use Case owners will then document and certify their compliance with the minimum risk management practices annually through the AI Use Case Inventory process. If the CDAO and/or AISC determines that an AI Use Case is non-compliant, the AI Use Case owner must terminate the AI Use Case and to restart the AI Use Case, the owner of that use case must develop a compliance plan with the review and approval of M/SS/CfA. Additionally, the Department will require AI Use Case owners to submit updates on their compliance when a significant change occurs to the AI or the context in which the AI operates, including independent reviews and evaluation by the RAIO, AISC, or approved bureau-level evaluation bodies.

To facilitate implementation, the Department is developing additional risk management guidance for developers. The CDAO will engage its existing governance bodies and continue to socialize requirements through AI.State and the AI Communications and Training Working Group.

The CDAO is responsible for the implementation and oversight of requirements for rights-impacting and safety-impacting AI. AI Use Case owners are responsible for implementing requirements within their own projects, with guidance from the CDAO as needed.

Appendix A: AI Governance Bodies

Enterprise Governance Board (EGB):

The EGB is comprised of nine permanent members, who serve as voting members. All voting members have an equal vote.

Permanent Members:

- The Deputy Secretary of State for Management & Resources (co-chairperson)
- The Deputy Secretary of State
- The Under Secretary of State for Management (alternate chairperson in the absence of a Deputy Secretary)
- All other Under Secretaries of State
- A representative of the Secretary of State as determined by the Secretary.

Advisors and Observers:

When the EGB convenes as the AI Governance Board, the CDAO serves as vice chair. The Board's charter, which the EGB Secretariat maintains and updates, sets forth additional advisors to the Board and its governance structure in greater detail. Advisors and observers may change frequently depending on EGB meeting topics, for example, including the CIO on sessions related to AI.

AI Steering Committee (AISC):

Voting members of the AISC include:

- **Co-Chair**: M/SS/CfA: Center for Analytics
- **Co-Chair**: DT/ECISO: Enterprise Chief Information Security Office
- Bureau of Administration (A)
- Bureau of Budget and Planning (BP)
- Bureau of Consular Affairs (CA)
- Bureau of Democracy, Human Rights, and Labor (DRL)
- Bureau of Diplomatic Security (DS)

- Bureau of Economic and Business Affairs (EB)
- Foreign Service Institute (FSI)
- Bureau of Global Talent Management (GTM)
- Bureau of International Organization Affairs (IO)
- Bureau of Intelligence and Research (INR)
- Bureau of International Security and Nonproliferation (ISN)
- Office of the Legal Adviser (L)

Bureau of Political-Military Affairs (PM)

- Office of the Under Secretary for Public Diplomacy and Public Affairs (R)
- Office of Civil Rights (S/OCR)
- Office of the Science and Technology Advisor to the Secretary (S/TECH)