Department of the Interior

Artificial Intelligence Compliance Plan

Prepared by the Chief Artificial Intelligence Officer Jay McMaster

The Department of the Interior's (DOI/the Department) AI Compliance Plan builds on the Department's AI Strategy of integrating AI across our operations to enhance decision-making, automate processes, and improve efficiency while ensuring meaningful human oversight, intervention capabilities, and accountability. This plan aligns with federal directives, including the President's Executive Order (EO) 14179, "Removing Barriers to American Leadership in Artificial Intelligence," EO 14277, and Office of Management and Budget Memorandum M-25-21 "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust", emphasizing the importance of innovative and secure AI technology. The Compliance Plan focuses on reducing barriers to AI adoption, modernizing infrastructure and processes, and promoting innovation through partnerships. Additionally, it highlights the importance of data management and sharing, workforce development, and continuous improvement to ensure the safe and effective deployment of AI technologies. With these efforts, the Department will be able to meet our AI strategic goals to integrate AI for improved decision-making and efficiency, build responsible and transparent AI capabilities to safeguard data and public trust, and establish an AI-ready workforce through ongoing training and collaboration.

Governance and Leadership

Overall AI Governance Model

The Department's AI Strategy outlines the vision and goals of the Department as an agency leader in AI implementation. The Strategy will be executed collectively by various components within the Department, including a Department AI Governance Board for oversight and prioritization, a Department AI Program for technical guidance and coordination, and the Department Information Management and Technology Leadership Team (IMTLT) for broader coordination and facilitation. These three bodies will provide a coordinated approach to create an AI-ready workforce and develop secure, reliable AI applications, ensuring efficient and effective operations across all Bureaus and Offices.

AI Governance Board (AIGB)

The Department will establish an AI Governance Board that will act at the executive level to address agency AI activities and coordinate with the Chief Artificial Intelligence Officer (CAIO) Council to ensure alignment with government-wide AI initiatives and best practices. The AI Governance Board will be chaired by the Deputy Secretary and vice-chaired by the Chief AI Officer (CAIO). Members will include executive-level representatives from the Offices of Policy, Management and Budget, Solicitor, Chief Information Officer, Acquisition and Property Management, Human Capital, and Ethics. Membership will also include a rotating representative from a bureau, office, or functional area.

The Chair and Board will determine the frequency of meetings and ensure that AI initiatives are aligned with departmental priorities, federal mandates, and ethical standards, and they are implemented safely and effectively across the Department. The Board will consult technical experts within and outside of the Department to broaden their perspective and integrate technical or sector-specific expertise, along with methods for engaging the workforce.

Department Chief AI Officer

The Department has established a CAIO position to promote responsible innovation, adoption, and governance of AI across the Department. The CAIO will play a central role in ensuring that AI is used in a manner consistent with legal requirements and government-wide guidance, working closely with other government officials to maintain compliance. As the senior advisor on AI in the Department, the CAIO will provide strategic counsel and participate in executive decision-making forums. In addition to internal leadership, the CAIO will represent the Department in external AI-related bodies, such as OMB-convened councils, standards organizations, governance boards, and international forums to align AI efforts across the federal government.

A key responsibility of the CAIO will be tracking AI use cases and overseeing the management of high-impact AI applications. High-impact AI use cases are defined by OMB M-25-21 as those whose output serves as a principal basis for decisions or actions that have legal, material, binding, or significant effect on rights or safety. This responsibility includes establishing processes to identify and document high-impact use cases, monitor their performance, evaluate effectiveness, and ensure risk management practices are in place. The CAIO will also be responsible for implementing an independent review process for these use cases prior to risk acceptance and for tracking them centrally.

Beyond governance, the CAIO will help guide the transformation of the Department workforce into one that is AI-ready, ensuring that staff are equipped with the necessary tools, skills and knowledge. The CAIO will coordinate with the CAIO Council and other federal agencies to leverage government-wide training programs and shared AI capabilities. The CAIO will also oversee the proper inventory, sharing, and release of custom-developed AI code and datasets. Furthermore, the CAIO will monitor evolving AI technology trends to advise on AI-related investments, helping the Department understand the resourcing needs required to implement AI initiatives effectively, and will support efforts to track AI-related spending across the department.

AI Program

Under the OCIO and CAIO, the Department will launch a centralized AI Program that will serve as the technical and strategic hub for AI activities. The AI Program will coordinate training, communication, oversight, and application development, providing recommendations on resources, monitoring compliance with M-25-21 and Office of Management and Budget Memorandum M-25-22 “Driving Efficient Acquisition of Artificial Intelligence in Government” timelines, and continually advising the AI Governance Board on policies to ensure that AI innovations remain safe, effective, and aligned with Department’s goals.

Bureau and Office AI Coordinators

The success of the AI Program hinges on the collaboration with Bureau and Office AI Coordinators, who will act as the primary points of contact for AI activities within their respective organizations. These coordinators, working alongside data stewards and information technology leadership, will manage AI use cases, manage risk assessments, support performance audits, and ensure effective implementation and management on the ground.

Implementation and Oversight

Together, the The AI Governance Board, CAIO, and the AI Program will work in tandem to implement AI across the Department, providing guidance and risk-management guardrails, tracking AI use-case inventories, and ensuring that high-impact systems undergo rigorous risk impact assessments and periodic performance audits before and after they are operational. This collaboration will be bolstered by the AI Community of Practice and expertise across the Department, facilitating procedures and standards, expanding partnerships, and building workforce proficiencies.

The AI Governance Board and the AI Program will also coordinate with other Department

governance boards to implement AI policies that emphasize data integrity, data integration, code sharing, and workforce development for emerging science and technology needs. By working closely together, these bodies will ensure a cohesive approach to AI governance within the Department.

Innovation Enablement

The Department must adopt a pro-innovation mindset, moving away from risk-averse approaches, to effectively leverage emerging technologies for government modernization and identify and remove unnecessary and bureaucratic requirements that hinder responsible AI innovation and adoption.

Reduce Barriers to AI Adoption

Empower AI Leadership: The Department will enable AI leaders, like the Chief AI Officer (CAIO), and AI champions to act as change agents and advocates for AI. AI leaders will promote department-wide AI innovation and address IT infrastructure, data access, governance, workforce development, and policy barriers.

Transforming Mindsets: New policy and guidance encourage American AI innovation to boost efficiency and productivity. We are experiencing a fundamental shift from a risk-averse stance to one that supports and embraces AI innovation. The Department will need to create flexible, resource-rich environments for AI users and developers, minimizing regulatory burdens. We are also undergoing a shift with operational commercial Large Language Models (LLMs), like general-purpose chatbots, becoming a relevant and accessible AI tool for end users. Unlike traditional methods which define use cases before building solutions, commercial and open chatbots focus on deployment first, then advocate effective use, allowing users to discover use cases. The Department will encourage the use of these new tools and support a shift in development and operations to take advantage of AI's capabilities.

Communications and Messaging: The term "AI" has various meanings, causing skepticism and confusion. The Department will create an educational campaign to clarify AI definitions and tools; show the value with Department-specific examples (e.g., generating draft funding proposals or reviewing thousands of grant applications); manage expectations and ethical use of AI (e.g., the need for humans in the loop to review and accept); and promote AI tool usage.

Enabling Cross-Functional Teams: The Department will establish internal teams that help our mission staff and technical expertise overcome barriers and learn how to integrate AI into their approach.

Modernize Infrastructure and Processes

Modernizing IT infrastructure and refining processes are fundamental to supporting scalable and efficient AI innovation and adoption across the Federal Government.

AI Platforms: The Department must ensure its people have access to adequate IT infrastructure, including computing resources specialized for AI. Providing AI developers with access to software tools, open-source libraries, and robust deployment and monitoring capabilities is necessary for rapid AI application development, testing, and maintenance. Prioritizing the migration of workloads to integrate with Department-designated Major Tiered Data Centers and commercial cloud hosting services will accelerate integration with the AI platforms.

Data Platforms: The Department will advance capacity to share, curate, label, and govern agency data to support training, testing, and operating AI. This effort involves maximizing appropriate access to both internally held quality data and agency data available to third parties. Embracing a strong metadata practice with rich semantics will improve the accuracy of AI that relies on our data and enable efficient automated risk management at scale.

Process Automation and Digital Modernization: AI can revolutionize government operations by improving efficiency of business and operational processes and strengthening customer service. Bureaus and Offices are encouraged to leverage AI to modernize legacy systems and assist with documentation, testing, and code transformation. It will be essential to continuously refine and evaluate these systems to ensure they continue to align with operational goals.

Policy Updates: The Department previously provided guidelines on Risk Managed Use of Generative AI (August 2023) and these guidelines will remain in effect as the Department refines additional guidance in alignment with M-25-21. The Department will revisit and update internal policies on IT infrastructure, data, cybersecurity, cloud, and privacy to align with federal AI guidance and relevant executive orders, as required by OMB M-25-21.

Cross-Discipline Acquisition Teams: The Department will work to update acquisition processes for AI to ensure alignment with OMB M-25-22. Collaboration and engagement from Bureau/Office leadership with varied expertise (e.g., IT, legal, privacy, procurement) are critical throughout the AI acquisition process to address potential issues early. This cross-functional approach ensures comprehensive consideration of risks and opportunities.

Applied Research in AI

The Department will actively engage in, and support applied research in AI to develop specific agency applications that advance the mission and address national challenges.

Strategic Research & Development: The Department will look at applying and testing new AI technologies to support mission delivery, aligning with national AI strategies and priorities. Though basic research is usually out of scope, developing AI applications within the agency is crucial to keep up with AI advancements. Applied research and testing are necessary to identify the best generative AI tools for code assistance, ensuring an effective, cost-efficient, and secure approach before department-wide implementation.

Prototyping and Trials: The Department will encourage AI system prototypes and trials, developing testable requirements to ensure ethical and responsible AI. The Department will share prototype results, code, models, and methods to enhance common business practices.

Focus on Trustworthy AI: Applied research should aim to create AI systems that are traceable, well-tested, privacy-conscious, and free of inappropriate biases. These systems should be transparent and explainable. Trustworthiness must be maintained throughout the AI lifecycle, from ideation

Innovation through Partnerships

to prototyping and final operation. This focus on trust should be a core part of AI innovation and adoption.

Collaboration across government, academia, industry, and civil society are essential to accelerate AI innovation and ensure responsible development and deployment. The Department will engage in collaboration with other federal agencies, higher education, and industry to ensure the effective application of new technologies to more effectively meet mission goals.

Federal Partnerships: Participation in AI working groups and initiatives, such as the U.S. National Science Foundation's National AI Research Resource (NAIRR) Pilot and the Office of Science and Technology Policy (OSTP) National Science and Technology Council (NSTC) Committee on Science and Technology Enterprise (CSTE) Networking and Information Technology Research and Development Program (NITRD), as well as the use of Cooperative Research and Development Agreements (CRADAs), can help the Department stay up to speed with and enable innovation using new AI technologies. The Department will also explore innovated funding opportunities such as the U.S. General Services Administration's Technology Modernization Fund (TMF) and others to support the rapid implementation of AI in the Department.

Public-Private Partnerships: The Department will look at public-private partnerships with leading AI industry organizations and academic institutions to craft technological solutions that meet Department specific needs. These partnerships can also contribute to supporting AI education. These partnerships are crucial for advancing American AI infrastructure and innovation.

Open-Source and Data Sharing: The Department will explore joint efforts to scale AI opportunities and responsibly share custom-developed AI code and data used to develop and test AI across the Federal Government and with the public. Open-source projects are seen as crucial for accelerating AI innovation by democratizing access to ideas, encouraging new ways of thinking, and creating communities to enhance understanding of AI systems.

Facilitate External Collaboration: The Department will work to allow, under safe security protocols, external partners and collaborators access to Department AI development and delivery platforms, regardless of whether they are on a Department network, or have access to government-furnished equipment.

Promoting Public Trust in the Department's Use of AI through Risk Management

The Department will develop a risk management strategy to serve as a strategic and operational tool for aligning cybersecurity protocols, privacy protections, risk governance, and lifecycle management with federal guidance, including the National Institute of Standards and Technology (NIST) AI Risk Management Framework and OMB Memorandum M-25-21. The plan will enable staff to evaluate, deploy, and monitor AI technologies while safeguarding sensitive data, minimizing unintended outcomes, and ensuring that AI-driven decisions align with the Department's mission and values.

Governance and Strategic Alignment

As AI technologies are integrated into the Department's daily operations and business services, clear roles and responsibilities, cross-functional coordination, and executive leadership become critical. Without strong governance, AI adoption risks becoming fragmented, non-compliant, or misaligned with legal and ethical standards. As part of the risk management strategy, the Department will:

- Form an AI Safety Board with broad representations from OCIO and mission Bureaus and Offices to provide oversight and direction related to AI risk decisions.
- Integrate the NIST AI Risk Management Framework into Department cybersecurity, privacy, procurement, and data governance strategies.
- Ensure strategic use of existing tools like the Bison Governance, Risk, and Compliance platform to support transparency and traceability of AI usage.
- Establish an agency-wide understanding of acceptable risk, including conditions for waivers or system denials.
- Conduct an agency-wide review of risk tolerance for high-impact AI.
- Publish criteria for acceptable risk, waiver conditions, and non-approval thresholds.
- Reassess risk tolerance annually or in response to changes in technology or mission priorities.

Risk-Informed Lifecycle Integration

Embedding AI-specific risk management into the Department's existing business and IT processes is essential to making risk evaluation a continuous and practical component of daily operations.

Policy and Intake Modernization: Modernizing policies and intake processes is a critical first step in ensuring that AI systems entering the Department environment meet baseline expectations for security, functionality, and alignment with mission needs. As AI systems can behave

unpredictably or produce unintended consequences, it is essential that the Department implement a robust pre-deployment testing and assessment process.

The Department will:

- Update existing policies to reflect AI-specific controls (e.g., NIST Security and Privacy Controls for Information Systems and Organizations (SP 800-53) updates for AI).
- Improve intake processes by encouraging reuse of secure, authorized systems before new acquisitions.
- Promote "secure-by-default" configurations for customer-built AI solutions.

Pre-Deployment Testing and Assessment: To ensure AI systems perform as intended and uphold the Department's standards for trust, transparency, and accountability, rigorous pre-deployment testing is essential. These assessments not only verify the technical soundness of AI models but also help identify potential risks before they can impact operations, security, or the public. The Department will develop standardized AI pre-deployment test plans with risk mitigation strategies using the MITRE ATLAS Framework for adversarial testing, vendor-native tools, and commercial testing platforms. The Department will also require AI Impact Assessments (AI-IAs) for all high-impact AI systems which will include independent internal reviewers and updated throughout the system lifecycle linked to waiver tracking and public transparency plans.

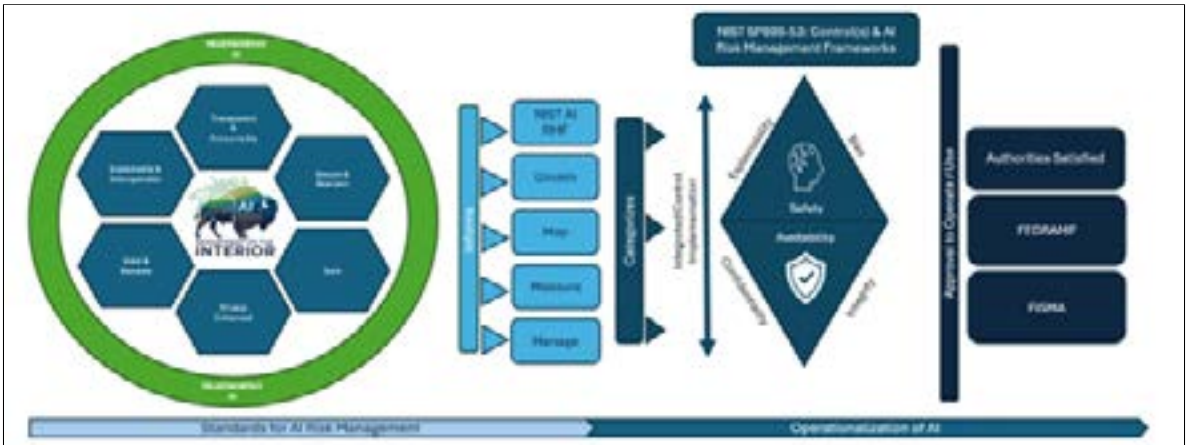

Figure 1. DOI AI Risk Management Compliance

High-Impact AI Risk Management Practices

For "high-impact" agency uses of AI, including those whose output may serve as the principal basis for decisions or actions that have legal, material, binding, or significant effect on rights or safety, the Department will implement risk management practices as required by OMB M-25-21, including:

- Meaningful human oversight, intervention, and accountability for all high-impact decisions.
- Pre-deployment testing and risk mitigation plans reflecting expected real-world outcomes and benefits to the intended use
- An AI impact assessment before deploying any high-impact AU use case
- Ongoing monitoring for performance and potential adverse effects
- Provision of adequate training and assessment for operators of AI

Operational Risk Management Infrastructure

As AI systems move from development into production, the Department will ensure that the operational environment supporting these systems is secure, resilient, and capable of managing evolving risks in real time. Operational risk management infrastructure provides the tools,

processes, and safeguards needed to monitor AI systems continuously, enforce security and privacy controls, and respond swiftly to anomalies or incidents.

Security, Privacy, and Authorization: Establishing a secure operational foundation for AI begins with enforcing strong security, privacy, and authorization controls tailored to the unique characteristics of AI systems. While traditional IT systems rely on established compliance standards, AI introduces dynamic behaviors, data dependencies, and model-specific vulnerabilities that require enhanced oversight.

The Department will:

- Align AI system security reviews with Federal Information Security Modernization Act (FISMA) and tailor controls from NIST SP 800-53.
- Include AI-related documentation in system acquisition (e.g., source code, model specs).
- Conduct privacy impact assessments (PIAs) for all AI systems handling PII.

Monitoring and Auditing: While establishing strong security and privacy controls is essential for authorizing AI systems, maintaining their integrity requires continuous oversight after deployment. AI models can drift over time, respond unpredictably to new data, or become vulnerable to emerging threats. To address these challenges, the Department will enable continuous performance monitoring, using available telemetry from AI systems; conduct periodic human reviews to validate legal, ethical, and security performance; and automate internal trend analysis and integrate with cyber incident response processes.

Use Case Inventory and Waiver Disclosure: The Department Chief Information Officer and CAIO will solicit input from all Bureaus and Offices on AI use cases for the annual inventory. A digital intake form will be created to collect the required information. Bureau and Offices will use the AI Coordinators to work across their organizations to ensure the inventory is complete and comprehensive. Updates to the inventory will be collected on a regular basis to ensure visibility into AI across the Department.

To ensure transparency and trust, the Department will release a public version of the inventory each year. The Department will also publicly release summaries and justifications for all AI risk waivers and the approvals and denials of high-impact AI use cases. This proactive disclosure ensures public awareness and accountability. Furthermore, in compliance with M-25-21, all non-compliant systems and waivers will be reported to the Office of Management and Budget (OMB) within 30 days.

Public Engagement and Feedback: Building on our transparency efforts, the Department will seek an avenue for public and customer input on AI use cases. This engagement involves developing or procuring an accessible interface for feedback, which will be synchronized with our internal use case tracking tools. This integration will enhance our responsiveness and provide a direct channel for continuous improvement based on valuable external perspectives.

Training, Awareness, and Human Oversight

Even the most sophisticated AI systems require informed human oversight to operate safely, ethically, and effectively. As AI becomes more deeply embedded in the Department of the Interior's daily operations, equipping staff with the right knowledge, skills, and responsibilities is essential to managing risk and maintaining trust. Human judgment remains a critical safeguard—ensuring that AI outputs are interpreted correctly, unintended consequences are identified early, and decisions remain accountable to our mission and the public.

AI-Specific Workforce Development

Equipping staff with the skills to understand and manage AI systems is only part of ensuring

responsible use, as equally important is establishing clear protocols for when and how humans must intervene. Training enables personnel to recognize when an AI system may be malfunctioning, biased, or operating outside its intended scope. The Department will incorporate AI risk training into annual Role-Based Security Training (RBST), and provide role-specific training for operators, risk managers, and reviewers of AI systems.

Fail-Safe and Human Intervention Protocols

The Department will build on the established foundation by defining operational safeguards, such as fail-safes and human-in-the-loop mechanisms, to ensure that AI systems remain under meaningful human control. These protocols will define mandatory fail-safe criteria for high-impact AI systems and document scenarios where fail-safes may be waived with proper approval and oversight.

Data Management and Sharing

AI systems depend on secure, high-quality, well-governed, actionable, and usable data as a strategic asset to generate accurate insights, drive automation, and enable intelligent decision-making. The following objectives will enable an AI-ready ecosystem that accelerates innovation and drives business across the enterprise.

Strengthen Enterprise Data Governance for AI

Effective data governance ensures that AI system data is accurate, consistent, secure, and responsibly managed. As the foundation of all AI models, high-quality data enables trustworthy outcomes and mission-aligned innovation. A robust data governance framework supports responsible data sharing and reuse across missions; clear policies for data quality, privacy, access control, and accountability; and compliance with federal laws and standards

To advance this governance, the Department will:

- Empower data leaders to manage agency data portfolios, collaborate across bureaus, and lead the adoption of mature data management practices that support AI readiness.
- Leverage the Department Data Governance Board to oversee policy adherence and resolve AI-related data issues.
- Appoint data owners and stewards across the organization to ensure data quality, accessibility, usability, compliance, and protection throughout the data lifecycle.
- Define and enforce data policies governing access, quality, usage, and regulatory compliance, while ensuring adherence to FAIR (Findable, Accessible, Interoperable, Reusable) principles.

Improve Data Quality and Fitness for Purpose

Improving data quality and fitness for use directly enhances the performance, reliability, scalability, and effectiveness of AI systems. High-quality data that is accurate, complete, timely, and relevant enhances the ability of AI models to learn patterns more effectively and ensure that solutions are mission-aligned. When data is well-prepared and fit for its intended purpose, it reduces errors, improves model accuracy, and minimizes the risk of faulty outputs, bias, or unintended consequences.

Ensure Data Quality and Consistency: The Department will implement automated data profiling, data cleansing practices and tools, and establish regular monitoring dashboards for reporting. The Department will define and implement processes for resolving data anomalies and inconsistencies at the source.

Operationalize Data Labeling and Annotation: The Department will build internal capability for data

labeling and annotation through automation. The Department will implement third-party platforms to scale this automation and standardize annotation formats to ensure interoperability across AI systems.

Incorporate Data Management Throughout the AI lifecycle: The Department will incorporate data management practices at each step in the AI lifecycle to enhance long-term data quality. A feedback pipeline will need to be established between the AI model and the data sources to allow for continuous improvement.

Champion Data Standardization through Data Standards: Standardization reduces duplication, minimizes errors, and enables efficient data integration. The Department will develop enterprise data standards for key data assets to ensure consistency, quality, and interoperability; ensure a common framework for data collection, storage, labelling, sharing, and model training; and align with record management policies and best data management practices, including data deprecation and archiving.

Utilize Data Analytics for Long Term Value: The Department will implement continuous monitoring and evaluation of AI models through advanced analytics to detect performance drift, biases, or inefficiencies to improve data quality.

Enhance Data Discovery, Access, and Sharing

An enterprise, modernized architecture with a centralized marketplace enhances data discovery, access, and sharing for AI by creating an environment where data is easier to find, trust, and use across the organization. A modern architecture supports scalable cloud services, APIs, and data catalogs that facilitate secure sharing across departments and with external partners, while enforcing compliance with privacy and security requirements. This approach reduces data silos, improves efficiency, and promotes collaboration, ultimately enabling faster development of AI models and more consistent mission-driven outcomes.

Build a Unified Data Architecture: The architecture will be based on open, machine-readable standards, and the Department will consolidate data into enterprise data lakes, warehouses, or other innovative solutions to enhance data's usefulness. Integration will occur across structured, unstructured, and semi-structured data sources. The Department will build on the current metadata management platform to track data lineage and improve discoverability through automation. Key data assets will include robust associated metadata following industry and government standards.

Develop a Centralized Marketplace: The Department will design and implement a centralized marketplace to list, showcase, and store (where appropriate) reusable, validated machine learning features. This marketplace should include data usage, performance, and version history.

Build Workforce Capacity in AI-Ready Data Stewardship

A well-trained and informed workforce is crucial to ensure data readiness, usefulness, and accessibility. Additionally, developing AI literacy and specialized skills across data stewardship roles ensures AI systems have responsible oversight for federal guidelines compliance and reduces risks related to misuse or other data deficiencies. To advance this capacity and stewardship, the Department will:

- Launch training programs on data stewardship, ethics, and quality best practices.
- Encourage cross-functional collaboration between data engineers and stewards, domain experts, and AI teams.

Ensure Privacy and Security of Sensitive Data

Securing sensitive data is foundational to any AI strategy and associated solutions to ensure compliance with regulatory and security requirements, prevent misuse, and encourage responsible innovation. To advance this effort, the Department will:

- Deploy role-based access controls (RBAC) for internal and external users. This includes applying data encryption, anonymization, and masking where appropriate to ensure data security.
- Identify and characterize sensitive data assets by utilizing automation tools.
- Utilize risk mitigation techniques by implementing auditing and logging on data access/use activities to meet regulatory requirements.

Workforce Development

The Department recognizes that the successful integration of AI into its mission-critical operations depends on a workforce that is not only technically proficient but also broadly AI literate. The Department is implementing a workforce development strategy that includes recruitment, training, retention, and the empowerment of both technical specialists and non-practitioners.

At the heart of this strategy is a commitment to cultivating a culture of continuous learning and innovation. The Department will coordinate with the CAIO Council to leverage government-wide training programs, participate in federal staff talent-exchange programs, and ensure all employees whose work could benefit from AI models have access to such tools. The Department aims to ensure that every employee, regardless of role, has the foundational understanding needed to engage with AI tools responsibly and effectively. This workforce strategy positions the Department to lead in the responsible and effective use of AI, ensuring that its people, not just its technology, are ready to meet the challenges and opportunities of the future.

Recruitment and Talent Acquisition: The Department will align its hiring strategy with the evolving demands of AI implementation. This includes identifying workforce gaps and recruiting individuals with expertise in data science, machine learning, AI ethics, and systems engineering.

Tiered Training and Upskilling: To ensure broad-based AI literacy, the Department is launching a tiered training model:

- Foundational AI literacy for all employees to build awareness and confidence in using AI tools.
- Specialist upskilling for data scientists, engineers, and analysts to deepen technical capabilities.
- Champion development to empower select individuals across bureaus to lead AI integration efforts and mentor peers.
- Training programs will be tailored to specific roles, ensuring relevance and applicability. These efforts will be embedded into existing professional development pathways and supported by digital learning platforms.

Retention and Empowerment: The Department is promoting an environment that supports career growth and innovation. This effort includes:

- Promoting cross-departmental collaboration and knowledge sharing among AI professionals.
- Recognizing and rewarding contributions to AI initiatives.
- Creating internal communities of practice to sustain momentum and build institutional knowledge.

Continuous Improvement

As part of our ongoing AI Strategy, the Department is committed to promoting a culture of continuous learning and improvement across all AI initiatives. This approach ensures our AI capabilities remain mission-aligned, ethically sound, and responsive to evolving federal standards, public needs, and technological advances.

To build a resilient and forward-looking AI program, the Department prioritizes workforce development by expanding AI understanding at all levels. Every employee plays a role in responsible AI use. Training programs will equip staff with the skills needed to apply ethical judgment, assess and mitigate risks, and innovate effectively. Feedback from employees, stakeholders, and end users is essential; Bureaus and Offices must implement mechanisms to collect, evaluate, and incorporate input to improve AI systems and address issues like faulty outputs or shifting user expectations.

Strong governance and thoughtful processes are vital to ensure our systems are trustworthy and effective. Bureaus and Offices should establish regular evaluations, real-world testing, and human reviews (at least annually or following any major updates) to detect any performance issues or unintended behaviors. For high-impact uses, Bureaus and Offices must conduct and update AI impact assessments documenting expected outcomes, risk profiles, and mitigation plans. These efforts should be integrated into the broader software development lifecycle through formal testing and evaluation activities.

Furthermore, maintaining and advancing our data and technology infrastructure is critical. Continuous improvement must be supported by high-quality, well-organized, and representative data. Bureaus should leverage automation and advanced analytics to identify workflow inefficiencies and accelerate operations. Infrastructure must support the full lifecycle of AI, including development, deployment, decommissioning, and monitoring. Additionally, contracts must protect our access to federal data to prevent vendor lock-in and support future enhancements. Tools like automated retraining pipelines, performance alerts, and documentation practices will help maintain transparency and accountability.

This approach ensures our AI capabilities remain mission-aligned, ethically sound, and responsive to evolving federal standards, public needs, and technological advances.

Implementation Timeline

The CAIO and AI Program will create a AI implementation action plan with milestones and timelines at the start of each fiscal year. This plan will provide transparency across the Department on the priorities for the year and progress towards the AI Strategy goals and objectives.

References

America's AI Action Plan. July 2025.

AI in Government Act of 2020, P.L. 116-260, 134 Stat. 2286-2291 (40 U.S.C. § 11301 note).

Executive Order 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," December 3, 2020.

Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," February 11, 2019.

Executive Order 14179 "Removing Barriers to American Leadership in Artificial Intelligence," January 23, 2025.

Executive Order 14277 "Advancing Artificial Intelligence Education for American Youth," April 23, 2025.

·Executive Order 14320, "Promoting the Export of the American AI Technology Stack", July 23, 2025.

Executive Order 14318, "Accelerating Federal Permitting of Data Center Infrastructure," July 23, 2025.

Executive Order 14275, "Restoring Common Sense to Federal Procurement," April 15, 2025.

Federal Data Strategy, "2020 Action Plan," December 2019.

John S. McCain National Defense Authorization Act for Fiscal Year 2019, P.L. 115-232, Sec. 238(g) (10 U.S.C. § 2358 note).

Office of Science and Technology Policy, "National Artificial Intelligence Research and Development Strategic Plan 2023 Update", May 2023.

National AI Initiative Act of 2020 (15 U.S.C. §9401 et seq.)

National Institute of Standards and Technology (NIST). "Artificial Intelligence Risk Management Framework 1.0 (AI RMF)," January 2023.

NIST, "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile", July 2024.

Office of Management and Budget (OMB) Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," April 3, 2025.

OMB Memorandum M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government," April 3, 2025.

U.S. Department of the Interior, "FY 2022-2026 Strategic Plan," 2022.

U.S. Department of the Interior Artificial Intelligence (AI) Website.

U.S. Department of the Interior AI Glossary.

U.S. Government Accountability Office (GAO) Report GAO21519SP, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," June 30, 2021.