DEPARTMENT OF LABOR
AI STRATEGIES
OFFICE OF MANAGEMENT AND BUDGET
MEMORANDUM M-25-21

PREPARED BY: MANGALA KUPPA,
CHIEF AI OFFICER, DOL
ISSUED BY: KEITH SONDERLING,
DEPUTY SECRETARY, DOL

Contents

1 AI USE CASES

The Department of Labor (DOL) is dedicated to using Artificial Intelligence (AI) to enhance the welfare of wage earners, job seekers, and retirees in the United States. The aim is to improve working conditions, increase employment opportunities, and ensure work-related benefits and rights. DOL aims to align AI investments with key use cases in enforcement, benefits programs, workforce development, compliance assistance, grants, and customer service, while driving innovation, promoting government efficiency, and protecting security, privacy, accessibility, and data confidentiality.

1.1 DOL AI Use Cases

DOL has implemented a range of mission-enabling AI use cases as well as general purpose enterprise uses of generative AI (GenAI) tools. Use cases include:

- Secure GenAI assistants and chatbots, AI enabled search assistants (including agency-specific AI assistants), enterprise shared AI use cases for large document analysis, document comparison, summarizations, and image analysis.

- Custom machine learning models to extract data from complex forms, identification of specific context in unstructured data through custom trained models, and redacting PII.

- Audio transcription, language translation, text to speech conversions, automated letter generations and secure note taking bots, and natural language processing tools for classification and summarization.

- Custom models for occupational coding, record matching, data classification, and predictive modeling. These systems support core statistical functions such as injury and illness classification, consumer expenditure analysis, and labor market data processing.

- AI coding assistants and agents in systems development and modernization activities.

DOL also intends to continue the use of AI to improve mission delivery to the American public. Below are a few examples of use cases under consideration for evaluation and proof of concept development.

- Deploy mission enabling AI like hands-free AI headsets to assist inspectors during field inspections. AI-enabled gear will capture video and audio, process inspection data, and generate documentation based on citations, orders, and regulations for human review.

Extract insights from documents or data and identify emerging trends. This has broad applicability across enforcement agencies. Use AI to support content discovery and knowledge management.

Help with records management tasks such as auto classification, meta data tagging, and search capabilities within records management life cycle activities.

Improve productivity with acquisition lifecycle tasks. This includes Statements of Work (SOW) draft creations, proposal evaluation assistance, and market research assistance.

Deploy and use AI applications in Rulemaking processes and Freedom of Information Act (FOIA) response automation.

Use agentic AI for back-office operations. This includes automating cyber operations, financial tracking and reporting, and eliminating manual tasks to free up staff time to focus on high value work.

Use AI to monitor grant performance or identify discrepancies in unemployment insurance monitoring program. Identify and detect fraud in benefits processing.

Tailor AI for use by legal professionals and use agentic AI to optimize tasks like contact center operations.
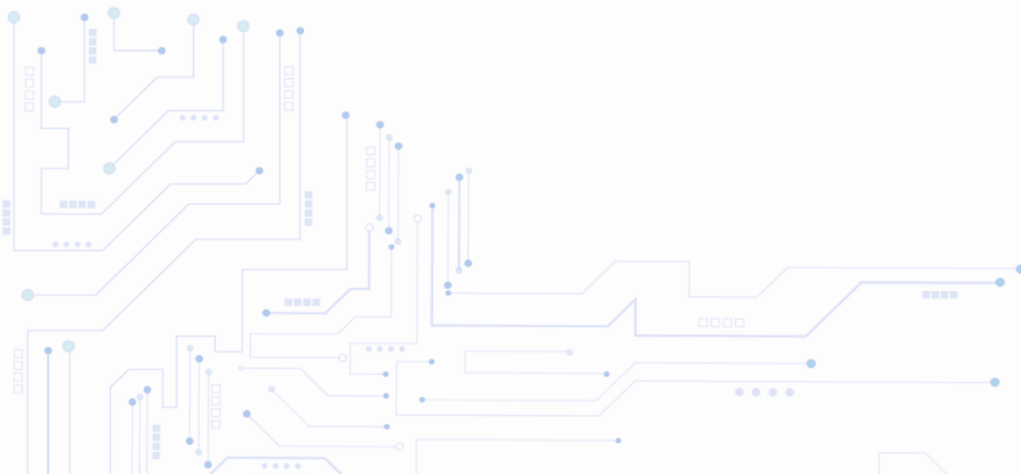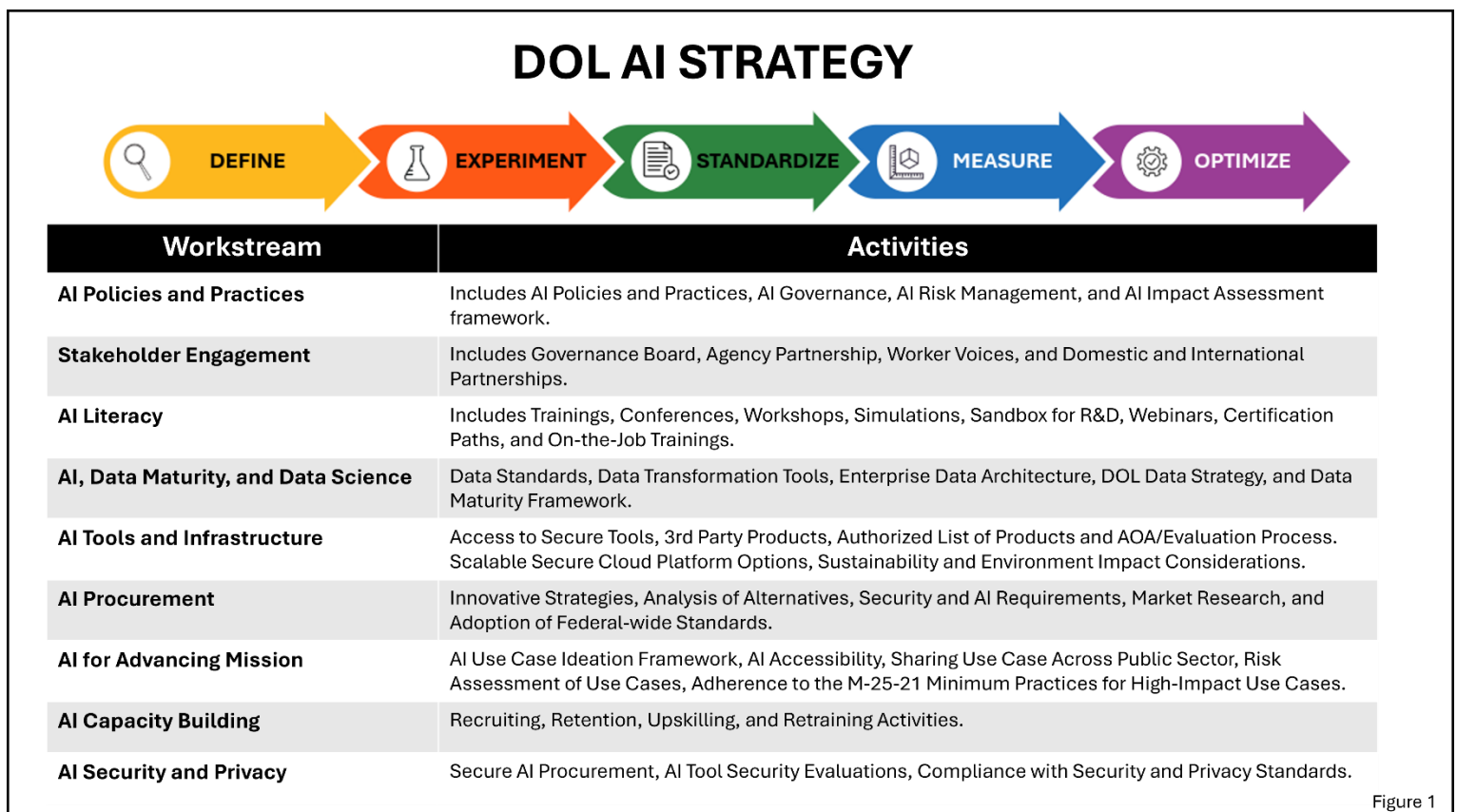
2 DOL AI Maturity Goals

The DOL AI strategy (Figure 1) consists of five maturity levels and nine parallel workstreams. While the maturity model provides a step-by-step progression — Define → Experiment → Standardize → Measure → Optimize — each workstream evolves at its own pace based on operational needs, resource availability, and strategic priorities.

This approach allows DOL to make incremental and targeted progress across multiple fronts simultaneously, rather than requiring uniform advancement across all areas. Once a workstream reaches the optimized stage, it transitions into a continuous improvement cycle to ensure sustained performance and adaptability.

DOL will conduct annual maturity assessments to evaluate progress, identify gaps, and refine strategies for each workstream. This ensures that the AI program remains responsive to emerging technologies, evolving risks, and mission needs.

DOL AI STRATEGY

DEFINE → EXPERIMENT → STANDARDIZE → MEASURE → OPTIMIZE

Workstream	Activities
AI Policies and Practices	Includes AI Policies and Practices, AI Governance, AI Risk Management, and AI Impact Assessment framework.
Stakeholder Engagement	Includes Governance Board, Agency Partnership, Worker Voices, and Domestic and International Partnerships.
AI Literacy	Includes Trainings, Conferences, Workshops, Simulations, Sandbox for R&D, Webinars, Certification Paths, and On-the-Job Trainings.
AI, Data Maturity, and Data Science	Data Standards, Data Transformation Tools, Enterprise Data Architecture, DOL Data Strategy, and Data Maturity Framework.
AI Tools and Infrastructure	Access to Secure Tools, 3rd Party Products, Authorized List of Products and AOA/Evaluation Process. Scalable Secure Cloud Platform Options, Sustainability and Environment Impact Considerations.
AI Procurement	Innovative Strategies, Analysis of Alternatives, Security and AI Requirements, Market Research, and Adoption of Federal-wide Standards.
AI for Advancing Mission	AI Use Case Ideation Framework, AI Accessibility, Sharing Use Case Across Public Sector, Risk Assessment of Use Cases, Adherence to the M-25-21 Minimum Practices for High-Impact Use Cases.
AI Capacity Building	Recruiting, Retention, Upskilling, and Retraining Activities.
AI Security and Privacy	Secure AI Procurement, AI Tool Security Evaluations, Compliance with Security and Privacy Standards.

Figure 1

➢ **Workstream 1 – AI Policies and Practices:** Enterprise AI adoption requires repeatable processes and practices for Governance, AI implementation, Risk Management, and Use Case Assessment. This work stream establishes the DOL AI strategy and ensures adoption of these standardized processes across DOL.

➢ **Workstream 2 – Stakeholder Engagement:** AI requires various DOL stakeholders to collaborate across technology, policy, program, security, privacy, and data dimensions. Given DOL's mission and goals, agency partnerships and employee engagement are also critical factors. This workstream defines various engagement activities and establishes a cadence and goals for each engagement. Additionally, engaging in the federal, academic, and private sector is crucial to keep up with the ever-changing AI landscape.

➢ **Workstream 3 – AI Literacy**: AI is still a novel technology and requires a strong AI literacy initiative for organizations to benefit from these tools and manage the risks from this technology. This workstream defines various options for increasing AI literacy across DOL.

➢ **Workstream 4 – AI, Data Maturity, and Data Science:** AI requires a strong data foundation for any meaningful use case implementations. DOL aims to establish enterprise data standards and tools aimed at data maturity across DOL. Working in collaboration with the Chief Data and Analytics Officer (CDAO), DOL will leverage the tools of data science to enhance the quality and integrity of DOL data assets.

➢ **Workstream 5 – AI Tools and Infrastructure:** AI innovation is only possible when DOL invests in securing various AI tools for DOL use. The tools must not present vulnerabilities and must follow federal and DOL security and data protection standards. This workstream aims to evaluate and establish secure access to authorized AI tools for DOL use for mission advancement. AI tools need robust and secure infrastructure to operate. DOL adopts a multi-cloud approach with a focus on supporting various DOL AI use cases. Additionally, DOL is focused on providing infrastructure for custom model development and deployment.

➢ **Workstream 6 – AI Procurement:** DOL intends to follow the guidelines established by the OMB/CAIO Council and any related workgroups. This workstream looks at standardizing the language for all AI procurement, conducting alternatives analysis, and market research for identification of the best acquisition strategies. This workstream also aims to identify innovative approaches to acquiring AI services, working in collaboration with the DOL Office of the Senior Procurement Executive. In addition, DOL aims to leverage OneGov acquisition channels and will fully comply with the OMB Memo M-25-22 guidelines.

- ➤ **Workstream 7 – AI for Advancing Mission:** DOL believes that the use of AI should benefit the American public and must advance the DOL mission. To achieve this, and to ensure AI use at DOL is secure, there must be a defined and repeatable way of identifying use cases, assessing impact of, and ensuring governance for AI use at DOL. This workstream aims to build this maturity. This also includes continuous monitoring of the performance of AI systems after the initial deployment.

- ➤ **Workstream 8 – AI Capacity Building:** DOL is focused on preparing the workforce for AI impacts as well as ensuring that the AI governance and implementation is led by a qualified AI workforce. This workstream aims to recruit, retain, and upskill the DOL workforce in these technologies.

- ➤ **Workstream 9 – AI Security and Privacy:** Security and privacy are paramount for AI. This workstream aims to follow the National Institute of Standards and Technology (NIST) and other federally recognized security best practices across the DOL enterprise. Privacy is reviewed for every use case with the DOL Privacy Office.

2.1 AI-Enabling Infrastructure

To support scalable and innovative AI development, DOL is enhancing its modern AI infrastructure footprint. This includes a FedRAMP authorized hybrid cloud AI workbench spanning multiple cloud providers, automated pipelines, centralized knowledge sharing, and robust testing and monitoring capabilities—all designed to accelerate delivery, enhance trust, and maximize impact.

Flexible AI Workbench

DOL's AI Job Enrichment Center is a centralized web portal that offers a hybrid cloud environment with modular tools and models, supporting a variety of vendors and easing adoption for various projects.

Community of Shared Knowledge

DOL established a centralized internal repository of AI assets—code, models, and data—that promotes reuse, reduces duplication, and fosters collaboration across mission areas.

Best Practices Across the AI Lifecycle

Traceability, explainability, and interpretability are embedded throughout the AI development process through the continuous adoption of best practices and tools.

AI Development Platforms

DOL established managed platforms that unify tools for data exploration, model training, and experimentation, with integrated version control and lineage tracking to support transparency and traceability.

Testing and Evaluation Infrastructure

DOL established controlled environments designed to evaluate AI systems against defined performance and reliability criteria, including stress-testing, red teaming, and adversarial testing.

Sandboxes

DOL has secure, pre-deployment environments that allow for the safe testing of high-impact AI systems — especially those affecting rights, safety, or access to services — prior to release into production.

Automated Continuous Integration and Continuous Delivery/Deployment (CI/CD) Pipelines

DOL established integrated pipelines that automate the transition from development to deployment, ensuring models are consistently packaged, validated, and released using standardized workflows. DOL will further enhance this with automated deployment pipelines that enable phased releases of AI models using risk-aware methods such as canary deployments, promoting safe and controlled rollout.

Containerization and Orchestration

DOL has container-based architecture using orchestration tools to ensure consistent, portable, and callable deployment across cloud and on-premises environments. DOL will further extend this for edge environments.

API Gateways

DOL established secure, standardized interfaces that enable internal and external systems to access AI capabilities reliably, with governance controls in place for monitoring and access management.

Automated Monitoring Tools

DOL uses cloud-based monitoring systems that track operational metrics—including accuracy, latency, and throughputs—and surface anomalies or failures in real time to support ongoing oversight. DOL will further invest in continuous model monitoring tools to automate detection of any drifts to maintain model accuracy and performance.

2.2 Data

The AI data enablement strategy ensures that AI systems are powered by high-quality, well-governed, and quality data. This framework strengthens collaboration between AI and data leadership, promotes stewardship, and supports interoperability, traceability, and accountability. By advancing enterprise data maturity, the strategy enables scalable, trustworthy, and mission-aligned AI outcomes.

Alignment with Enterprise Data Priorities

DOL AI initiatives are developed in close collaboration with the department's Chief Data and Analytics Officer (CDAO) to align with enterprise data strategies and advance overall data maturity.

Secure API Gateway for Data Access

A centralized API gateway enables secure, scalable access to internal datasets and supports appropriate interagency data sharing—facilitating efficient data integration.

Enterprise Data Governance

Enterprise-wide data governance processes ensure data stewardship, with a strong focus on quality, integrity, and ethical use throughout the AI lifecycle.

Data Sharing and Reuse

Standardized data sharing agreements and interoperable tools reduce duplication, increase collaboration, and accelerate time-to-value for AI initiatives.

Model Documentation and Transparency

Model cards are used to document the purpose, performance, limitations, and data lineage of AI models—enhancing transparency, explainability, and traceability.

Structured Model Evaluation

AI models are evaluated through a formal governance process, including performance assessments to ensure effectiveness, explainability, interpretability, traceability, and accountability.

Centralized Data Access via EDP

The Snowflake-powered Enterprise Data Platform (EDP) provides a centralized environment for curated data access, enabling real-time dashboarding, analytics, and informed decision-making across the organization.

Established Data Standards

Published data and ingestion standards for AI ensures consistency, interoperability, and quality across data systems—supporting scalable and trustworthy AI operations.

2.3 AI Ready Workforce

DOL recognizes that AI is rapidly evolving and requires foundational literacy. A dedicated workstream has been established to define and implement multiple pathways for increasing AI literacy across the department.

AI Literacy Platform:
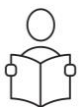
DOL has adopted a learning management platform to deliver curated AI training content, organized into learning paths tailored to Business, Executive, and Technical learners at Beginner, Intermediate, and Expert levels. The platform supports progress tracking and incentivization through digital badges and certifications.

Expanded Training Programs:

The CAIO office is collaborating with external partners to enable additional AI-focused courses. DOL plans to launch cohort-based technical training and career-track certification programs that allow staff to build AI skills aligned with their roles and goals.

Inter-Agency and Academic Training:

DOL participates in OPM/GSA-led training programs and leverages free offerings from academic institutions and private sector. The AI Job Enrichment Center publishes and promotes these opportunities to all DOL staff.

Empowering Non-Technical Staff:

AI literacy efforts include non-practitioners—program managers, policy analysts, and leadership—so they understand AI capabilities, risks, and governance principles. DOL is also investing in learning simulations as well as many community engagements to develop AI talent.

Talent Acquisition and Development:

DOL has identified and established AI skills necessary for the department. DOL also established standard Position Descriptions (PDs) for the new roles identified. These roles include both technical and non-technical tracks like the Data Science series. Additionally, DOL will leverage any federally available resources to attract talent. Recognizing the scarcity and competition for AI resources, DOL is also pursuing experienced IT Specialist staff to develop AI skills. Furthermore, DOL intends to recruit career ladder and college graduates to train them for AI jobs.

Job Detail Opportunities:

DOL plans to establish job rotation opportunities for hands on experience.

2.4 Research and Development

DOL operates internal sandbox environments that function as an AI innovation lab, enabling teams to prototype and evaluate AI tools in a secure, controlled setting; this capability acts as an AI accelerator to assess emerging technologies before broader deployment. The CAIO office continuously monitors emerging AI research and trends and engages appropriate partners, following governance and security protocols, to remain at the forefront of AI adoption.

DOL follows a process of hands-on research using trial versions, implementation of proof of concepts, and piloting new technologies to gather user feedback before full scale adoption.

2.5 Governance and Risk Management

DOL has developed a process to coordinate with key internal stakeholders, including the implementation of the DOL Use Case Impact Assessment Framework to manage risks associated with AI, particularly those deemed high-impact under OMB Memo M-25-21. DOL is committed to building enterprise capacity for AI innovation by institutionalizing strong governance, continuous risk management, and operational readiness.

2.5.1 AI Governance

DOL has established a centralized AI governance function with clearly defined roles, approval gates, and an authoritative inventory of AI and machine learning use cases, categorized by impact and risk.

DOL has also deployed an enterprise-grade ModelOps platform—a centralized system that manages the full lifecycle of AI and machine learning models. This platform enables:

✓ Model Registration and Version Control: Ensures traceability of models, including lineage, ownership, and change history.
✓ Automated Workflows: Standardizes development, validation, deployment, and retirement processes with embedded policy gates.
✓ Risk and Compliance Enforcement: Integrates testing protocols for accuracy, robustness, privacy, and security aligned with the NIST AI Risk Management Framework (RMF).
✓ Monitoring and Observability: Provides real-time dashboards, drift detection, and alerts for performance degradation or policy noncompliance.
✓ Audit and Documentation: Maintains immutable logs and model cards to support transparency, accountability, and regulatory reporting.

Testing, Evaluation, Validation, and Monitoring:

DOL has initiated processes for reusable test suites aligned with federal standards such as the NIST AI RMF. High-impact systems undergo independent validation with reproducible test results prior to deployment. DOL intends to further implement post-deployment continuous monitoring systems to track model drift, performance degradation, harmful outputs, and policy noncompliance using telemetry, alert thresholds, dashboards, and human-in-the-loop review mechanisms.

Security and Privacy:

Security and privacy are embedded by design. DOL conducts AI-architecture and solution reviews to enforce these standards. Our standard Systems Development Lifecycle (SDLC) is tailored for AI to include model selection, data readiness evaluation, and any specific privacy concerns based on the AI use case.

Audit, Compliance, and Accountability:

DOL conducts audits of AI systems prior to deployment, including design documentation, training data, outputs, and logs. These audits will assess alignment with OMB Circular A-130, M-24-10, NIST controls, and internal standards. Immutable audit logs will be maintained for all decisions, model changes, and monitoring outcomes. High-impact use cases will undergo independent review, and corrective action protocols will be supported by metrics and executive reporting to drive continuous improvement. This is repeated anytime there is a change that impacts the use case.

AI-Specific Incident Response:

DOL has a mature incident response process and is enhanced for AI specific incidents. Automated alerts, anomaly detection, and rollback or kill-switch capabilities will enable early risk detection. Escalation paths are being customized for business, privacy, cybersecurity, and legal teams. Post-incident reviews will inform updates to models, data pipelines, policies, and controls.

2.5.2 AI Risk Management

DOL's AI risk management approach is embedded within a centralized governance framework that spans the entire AI lifecycle—from development to decommissioning. Oversight is provided by a centralized CAIO team in partnership with Cybersecurity, Data, Privacy, and other relevant officials. Our Impact Assessment Frameworks ensures that all AI systems must be registered in a centralized inventory and assigned a risk tier based on impact, sensitivity, and operational criticality. No system may proceed without an approved risk classification. Governance policies are enforced through automated workflows.

High-Impact AI Determination:

AI use cases are reviewed to determine if they meet the definition of high-impact (i.e., those with significant effects on rights, safety, or access to critical services). This determination is documented and signed off by the CAIO representative and agency.

Minimum Risk Management Practices:

For high-impact AI, DOL implements the minimum practices outlined in OMB Memo M-25-21 Section 4(b), including:

- ✓ Pre-deployment testing and risk mitigation planning
- ✓ AI impact assessments covering purpose, data quality, civil rights implications, and independent review
- ✓ Ongoing monitoring for performance and adverse impacts
- ✓ Human training and oversight
- ✓ Fail-safe mechanisms and accountability structures
- ✓ Appeals and remedy processes
- ✓ Public feedback mechanisms

Internal Coordination Across Key Functions:

DOL's risk management strategy is built on strong internal coordination across key functional areas:

- ✓ Data Governance (Chief Data and Analytics Officer/Data Board): Ensures data quality, provenance, labeling, and access controls. Participates in early intake reviews to validate data readiness and compliance.
- ✓ Privacy Office (Senior Agency Official for Privacy): Leads privacy threshold analyses (PTAs), privacy impact assessments (PIAs), and ensures data minimization, de-identification, and alignment with the Privacy Act and E-Gov Act.
- ✓ Cybersecurity (Chief Information Security Officer/Information Systems Security Officer): Conducts AI-specific threat modeling, adversarial testing, and integrates AI control overlays into the Authority to Operate (ATO) process. Ensures compliance with NIST SP 800-53, 800-37, 800-171, and 800-218 Secure Software Development Framework (SSDF).
- ✓ IT and Enterprise Architecture (Office of the Chief Information Officer): Reviews technical fit, interoperability, and Section 508 compliance. Supports secure infrastructure and integration with enterprise systems.

Joint reviews are conducted at intake, and model changes trigger privacy and security impact checks. Approvals are recorded in the model registry, and continuous oversight is maintained through dashboards and alerts shared with the AI Governance team, the Security Operations Center, and the Privacy Office.

DOL has a defined process for authorizing AI tools and monitoring the use of AI tools to detect any unauthorized uses to prevent data leakage and protect DOL sensitive information. Our zero-trust architecture helps to easily identify and block such uses. This process is coordinated by the IT Operations unit and is carried out continuously as part of protection against potential AI use risks.

2.6 Resource Tracking and Planning

DOL has developed a use case ideation framework to uncover new opportunities. Additionally, user input and ideas are collected regularly through a centralized AI requests portal for building a pipeline of use cases for implementation. This framework involves:

Analyzing Current State Business Processes

This step starts with prioritized business areas for analysis, using multiple methods of collecting information including interviewing and documentation reviews, and using survey to collect information and user feedback on the current state.

Identifying Future State

This stage uses AI skilled consultants to review the business need and identify all opportunities of AI to improve operational efficiencies. This step also includes initial analysis of potential benefits, risks, and implementation level of effort for planning purposes.

Prioritizing Identified Opportunities

Once all the information is collected, the business unit uses this step to prioritize and shortlist agreed-upon initiatives for implementation with the CAIO office.

Tracking AI Investments

DOL has established a centralized reporting mechanism for quarterly updates to the CAIO office for oversight and planning.

Ensuring Effective Procurement of AI

DOL follows guidance set forth in the OMB Memo M-25-22 on AI procurement and has developed internal guidance for AI procurement, including standardized contract language addressing security, privacy, and performance considerations. DOL will further mature this from any guidance availed through the CAIO Council and workgroups.