Department of the Interior

Artificial Intelligence Glossary

Accountability: The obligation of individuals or organizations to explain, justify, and take responsibility for their actions and decisions, especially in the context of AI system development and deployment.

Algorithm: A clearly defined, step-by-step computational procedure for solving problems, performing calculations, or making decisions.

Artificial Intelligence (AI): "Artificial Intelligence," as defined in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, generally refers to the capability of machines or software to perform tasks that typically require human intelligence, such as reasoning, perception, language processing, and decision-making, and that can learn and adapt from data to improve performance.

AI High-Impact Risk Assessment: A structured evaluation process designed to identify, analyze, and mitigate potential ethical, societal, operational, or safety impacts of an AI system prior to and during its deployment.

AI Lifecycle: The sequence of stages in AI system development and management, including planning, data collection, training, deployment, monitoring, updating, and retirement.

Bias: Systematic and potentially unfair favoritism or discrimination introduced into an AI system through skewed data, algorithmic design, or human oversight, resulting in unintended outcomes.

Chief AI Officer (CAIO): A designated senior official responsible for overseeing and coordinating an organization's AI strategy, implementation, governance, and ethical compliance.

Data Governance: Policies, processes, and standards for managing data availability, usability, integrity, security, and privacy within an organization.

Deep Learning: A subset of machine learning that uses neural networks with multiple layers (deep neural networks) to model complex patterns in large datasets.

Explainability (Explainable AI): The capacity of an AI system to provide clear, understandable reasoning behind its outputs or decisions, facilitating transparency and trust.

The Federal Information Security Modernization Act (FISMA): A US federal law that requires federal agencies to develop, document, and implement information security programs to protect government information and operations.

Generative AI: A type of artificial intelligence that can understand, learn, and apply knowledge in a wide range of tasks, similar to human intelligence.

High-Impact AI Use Case: AI is considered high-impact when its output serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on rights or safety.

Machine Learning (ML): A type of AI that enables systems to improve performance over time by learning from data and experiences without being explicitly programmed for specific outcomes.

Model (AI Model): A mathematical representation trained on data that captures patterns, enabling predictions, decisions, or classifications on new inputs.

Natural Language Processing (NLP): An area of AI that enables computers to understand, interpret, and generate human language in spoken or written form.

Role-Based Access Control (RBAC): A security paradigm that restricts system access to authorized users based on their roles within an organization. It ensures that individuals can only access data and perform actions that are pertinent to their designated roles, thereby enhancing security and compliance.

Robustness: The ability of an AI system to maintain consistent and reliable performance under varied conditions, including unexpected inputs or adversarial conditions.

Transparency: The extent to which AI methodologies, data inputs, processes, and outcomes are openly documented and understandable to stakeholders.

Trustworthy AI: AI systems designed and implemented to respect human rights, privacy, fairness, transparency, accountability, and safety, encouraging trust and confidence from users and the public.

Training Data: Datasets used to teach or train an AI model, allowing it to learn patterns and generalize to make accurate predictions or classifications.

Use Case: A specific scenario or application in which artificial intelligence technologies are employed to solve a problem, automate a process, enhance decision-making, or deliver value within a particular domain or context.

Validation and Verification (V&V): Methods used to ensure that an AI system meets intended requirements (verification) and fulfills its intended purpose in real-world scenarios (validation).

Unsupervised Learning: A machine learning technique where the model is trained on unlabeled data, identifying patterns and relationships without explicit guidance on what to learn.