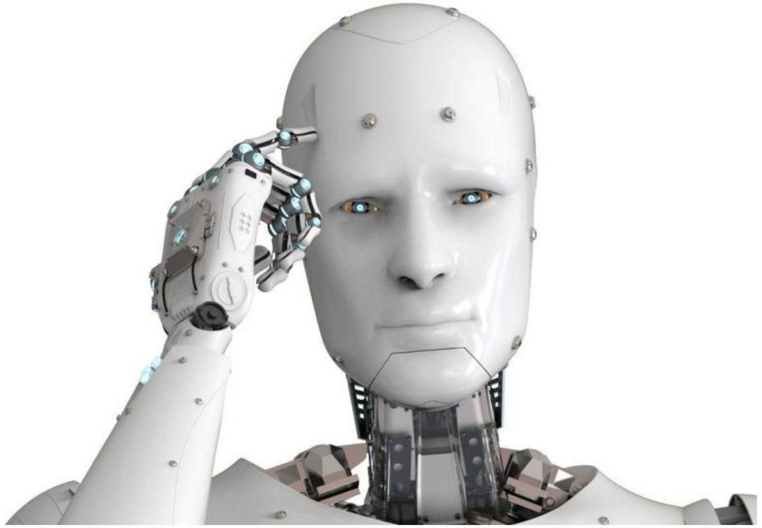
McCarter & English

Artificial Intelligence in the Federal Government

What is Artificial Intelligence (”AI”)?

- A field of study to develop and study the intelligence of machines and software, as opposed to the intelligence of humans or animals
- Software programs coded to solve problems through the ingestion of large data sets
- Examples: digital assistants, self-driving cars, chatbots, and facial recognition



Evolution of AI in Federal Government

- E.O. 13859, *Maintaining American Leadership in Artificial Intelligence* (Feb. 11, 2019)
  - Sustain and enhance U.S. position in AI R&D and deployment through a coordinated federal government strategy
- E.O. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Dec. 3, 2020)
  - Encourages agencies to use AI when appropriate and directs OMB to develop policy roadmap to support use of AI
- Identifying Outputs of Generative Adversarial Networks (IOGAN) Act
  - Directs National Science Foundation to support research on manipulated or synthesized content and information security (deep fakes)
- Artificial Intelligence in Government Act of 2020
  - Directs GSA to create an AI Center of Excellence to facilitate the adoption of AI technologies in federal government and OMB to develop guidance on AI's use in federal government
- National Artificial Intelligence Initiative Act of 2020
  - Coordinate ongoing AI research, development, and demonstration activities and provide sustained and consistent support for AI R&D
- Advancing American AI Act (NDAA FY 2023)
  - Tasked OMB with developing guidance to ensure acquisition of AI aligns with guidance OMB issued under the AI in Government Act of 2020 and developing an AI Hygiene clause to protect government information, privacy, civil rights, and civil liberties

AI Defined in the Federal Government: An Evolution

NDAA for FY 2019 defined AI to include the following:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances ***without significant human oversight***, or that can learn from experience and improve performance when exposed to data sets

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action

(3) An artificial system ***designed to think or act like a human***, including cognitive architectures and neural networks

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task

(5) An artificial system ***designed to act rationally***, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting

From National Artificial Intelligence Initiative Act of 2020 and used in E.O. 14410, AI is defined to mean:

A machine-based system that can, for a given set of human-defined objectives, ***make predictions, recommendations or decisions influencing real or virtual environments***. Artificial intelligence systems use machine and human-based inputs to-

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options for information or action

15 USC § 9401(3)

E.O. 14110, *Safe, Secure and Trustworthy Development and Use of Artificial Intelligence* (Oct. 30, 2023)

- The benefits AI presents must be balanced by the societal harms it could exacerbate if used irresponsibly
- Development and use of AI governed by eight principles and priorities:
  1. AI must be safe and secure
  2. Promote responsible innovation, competition, and collaboration
  3. Commitment to supporting American Workers
  4. AI policies must be consistent with advancing equity and civil rights
  5. Protect the interests of Americans who increasingly use, interact with, or purchase AI-enabled products
  6. Protect American's privacy and civil liberties
  7. Manage risks from federal government's own use of AI
  8. Federal government should lead the way

E.O. 14110: Section 4, *Ensuring the Safety and Security of AI Technology*

- Directs NIST to develop guidelines, standards, and best practices for AI safety and security
- Ensuring safe and reliable AI by requiring Secretary of Commerce to propose regulations for:
  - Companies to report on ongoing or planned activities to train, develop, or produce dual-use foundation models, including physical and cybersecurity protections
  - U.S. IaaS providers to submit reports when a foreign person transacts with the U.S. IaaS provider to train large AI models with the capability to be used in malicious cyber-enabled activity
- Assess potential risks related to use of AI in critical infrastructure sectors
- Reduce risks at the intersection of AI and CBRN Threats
- Reduce risks posed by synthetic content (deep fakes)

E.O. 14110, Section 5: *Promoting Innovation and Competition*

- Attract AI Talent to the United States
- Promoting Innovation
  - National Science Foundation
  - Health and Human Services
  - Department of Energy
- Promoting Competition
  - Support small business innovation and commercializing AI
    - "Small Business AI Innovation and Commercialization Institutes"
      - ❑ What this is has not been explained

E.O. 14110, Section 10: *Advancing Federal Government Use of AI*

- Director of OMB shall:
  - Provide guidance on federal government use of AI within 150 days of the date of the E.O.
- Facilitate agencies' access to commercial AI capabilities
  - GSA coordinate on taking steps to facilitate access to federal government-wide acquisition solutions for specified types of AI services and products

What’s on the Horizon for AI

AI.gov

- Launched in May 5, 2021
- Provides public with information on federal government activities advancing the design, development, and responsible use of trustworthy AI
- Includes policy documents, strategies, applications of AI, and updates on activities related to the National AI Initiative
- Provides a list of the government’s current use of AI
  - Over 700 AI uses across federal government as of September 1, 2023
- Possible opportunities from these use cases?

DoD: *Data, Analytics, and Artificial Intelligence Adoption Strategy* (Nov. 2, 2023)

- Builds upon and supersedes DoD’s 2018 AI Strategy and 2020 Data Strategy to continue DoD’s digital transformation
- Purpose of 2023 Strategy:
  - Leverage high-quality data, advanced analytics, and AI to enable DoD leaders and warfighters to make rapid, well-informed decisions
  - Focus on utilizing commercial solutions to ensure DoD’s capability pipelines address evolving requirements while balancing protection of industry intellectual property

OMB, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Mar. 28, 2024)

- Memorandum directs agencies to advance AI governance and innovation while managing risks from the use of AI in federal government
- Applies to new and existing AI developed, used, or procured by or on behalf of covered agencies
- Establishes agency requirements and guidance including:
  - **Strengthening AI governance:** Agencies must designate a Chief AI Officer to promote AI innovation and manage AI risk within the agency

OMB: Advancing Responsible AI Innovation

Advancing Responsible AI Innovation:

- Agencies must must develop and publicly release a strategy for identifying and removing barriers to the responsible use of AI and achieving enterprise-wide advances in AI maturity
- Create internal environments to promote AI innovation and risk management, paying special attention to:
  - Adequate ***IT Infrastructure***
  - Develop adequate infrastructure and capacity to sufficiently curate agency ***datasets*** for use in training, testing, and operating AI
  - Update, as necessary, ***cybersecurity*** authorization processes to better address the needs of AI applications

Managing Risks from the use of AI:

- Implement risk management practices to safety-impacting or right-impacting AI or else terminate non-compliant AI
- Comply with forthcoming documentation requirements prepared by OMB that should be required from a selected vendor in the fulfillment of a federal AI contract

OMB: Managing Risks in Federal Procurement of AI

Procurement of AI shall adhere to forthcoming guidance and the following principles:

- Align with applicable laws
- Ensure transparency and adequate performance of procured AI
- Promoting Competition in Procurement of AI
- Maximizing the Value of Data for AI
- Overfitting to Known Test Data (not limiting AI system training only to test data)
- Responsible Procurement of AI for Biometric Identification
- Responsibly Procuring Generative AI
- Assessing for Environmental Efficiency and Sustainability

The Open End of AI

Discussions are really just starting in earnest

- Data training sets
    - Government- or proprietary-data and allocation of rights therein
- Keeping pace with industry
- AI design/”AI-BOM”?
    - Need for AI-specific SBOM requirement?
- Just how much detail in what type of procurement?
- Will procurement policies lead the way in responsibly regulating AI?

Questions? We are here to help!

Cara Wulf

Partner

McCarter & English LLP

202-753-3401

cwulf@mccarter.com

Philip Lee

Associate

McCarter & English LLP

202-741-8209

plee@mccarter.com