McCarter & English

Public Contracting Institute

Artificial Intelligence Means Real Money: What Government Contractors Need to Know About the AI Revolution

Alexander W. Major, Esq.
Philip Lee, Esq.

February 22, 2024

Who are we?

- Attorneys in the Government Contracts and Export Controls Group at McCarter & English
- Significant experience handling “bet the company” litigation, investigations and bid protests
- Clients range from Fortune 100 companies to small businesses
- Extensive experience in defense and civilian contracting across multiple industry sectors

Today's Agenda

- Introduction
- AI in the federal government
- Federal guidance regarding AI
- Biden's Executive Order ("E.O.") 14110
- What's On The Horizon?

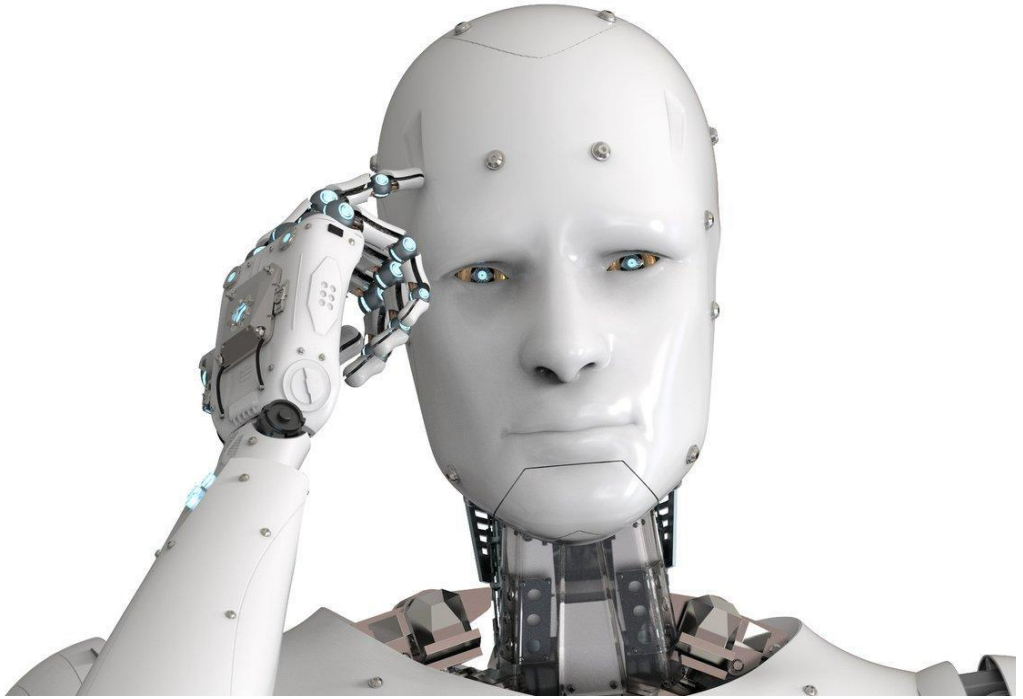
McCarter English

Introduction

Welcome to the Rabbit Hole

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



M&E Public Contracting Institute

AI Defined in the Federal Government: An Evolution

In 2019, AI defined 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

Under the Biden E.O., 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

McCarter English

AI in the 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 guided by five principles:
  1. Drive technological breakthroughs in AI to promote scientific discovery, economic competitiveness, and national security
  2. Drive development of appropriate technical standards and reduce barriers to safe testing and deployment
  3. Train current and future generations of American workers with necessary skills
  4. Foster public trust and confidence in AI technologies
  5. Promote an international environment that supports American AI research and innovation

E.O. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Dec. 3, 2020)

- Builds upon E.O. 13859 and encourages agencies to use AI when appropriate
- Provides additional principles agencies shall adhere to when designing, developing, acquiring, and using AI in the federal government
- Directs OMB to develop a policy roadmap on guidance OMB intends to create to support the use of AI
- Requires agencies to inventory non-classified and non-sensitive AI use cases and develop plans to ensure AI applications are either consistent with the E.O. or retired

Identifying Outputs of Generative Adversarial Networks (IOGAN) Act

- Gaps exist on research needed to develop tools that detect videos, audio files, or photos that have manipulated or synthesized content
- Required Director of National Science Foundation to support research on manipulated or synthesized content and information security
- “Deep Fakes”

M&E Public Contracting Institute

Artificial Intelligence in Government Act of 2020

- Required Administrator of GSA to create an AI Center of Excellence that would:
  1. Facilitate the adoption of AI technologies in the federal government;
  2. Improve cohesion and competency in the adoption and use of AI within the federal government; and
  3. Regularly convene to discuss recent developments in AI and disseminate information regarding programs, pilots, and other initiatives at agencies on the understanding, adopting, and use of AI

National Artificial Intelligence Initiative Act of 2020

- Initiative established to coordinate ongoing AI research, development, and demonstration activities
- Provide sustained and consistent support for AI R&D through grants, cooperative agreements, testbeds, and access to data and computing resources
- Initiative sunsets 10 years after date of enactment (end of CY 2030)
- New definition provided for AI:
  - 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

Advancing American AI Act (NDAA FY 2023)

- Directed DHS to develop policies and procedures related to the Department's acquisition and use of AI, including consider the risk and impacts related to AI-enabled systems
- Tasked Director of OMB with developing an initial means by which to ensure contracts for the acquisition of AI aligns forthcoming guidance OMB required to issue under Section 104 of the AI in Government Act of 2020
  - Develop an "**AI Hygiene Clause**" within 1 year of Act's enactment
  - Identify 4 use cases for the application of AI-enabled systems to
    - Support interagency or intra-agency modernization initiatives and
    - evaluate risk and develop a mitigation plan in utilizing AI systems

McCarter English

Federal Guidance Regarding AI

OMB M-21-06, *Guidance for Regulation of Artificial Intelligence Applications* (Nov. 17, 2020)

- Prepared in response to E.O. 13859, *Maintaining American Leadership in Artificial Intelligence*
- Sets forth policy considerations to guide AI applications developed and deployed **outside** the federal government
- Agencies directed to:
  - Avoid regulatory and non-regulatory actions that needlessly hamper AI innovation and growth
  - Consider new regulation only after deciding that it is necessary
- 10 regulatory and 4 non-regulatory principles to guide agencies

GSA AI Center of Excellence

- Created pursuant to the AI in Government Act of 2020
- Designed to assist modernizing agency infrastructure based on best practices
- Incorporates machine learning, neural networks, intelligent process design and Robotic Process Automation (RPA) to develop AI solutions that address agency challenges
- Agile-focused: Lean innovation to experiment and iterate quickly while identifying important use cases within an agency

GSA AI Center of Excellence (cont'd)

Supports agencies with the following services:

- **Governance and enablers assessment:** Assess agency's preparedness to explore AI solutions and create organizational support structures to grow and scale a mature AI program
- **Use case discovery and selection:** Identify opportunities for AI development efforts
- **Process automation and workflow mapping:** Define as-is business processes to understand human and machine touch points across workflows and leverage intelligent processes to collect more accurate and reliable data
- **Lean innovation process design:** Establish business processes and acquisition tools to scale AI initiatives from pilot to enterprise solutions
- **Identification and implementation of AI solutions:** Identify and implement technical solutions to address challenges by using AI techniques

WH OSTP, *Blue Print for an AI Bill of Rights* (Oct. 2022)

- Provides a framework based on five principles to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of AI
  1. Safe and effective systems
  2. Algorithmic discrimination protections
  3. Data privacy
  4. Notice and explanation
  5. Human alternatives, consideration, and fallback
- Technical companion of practices to implement the five principles

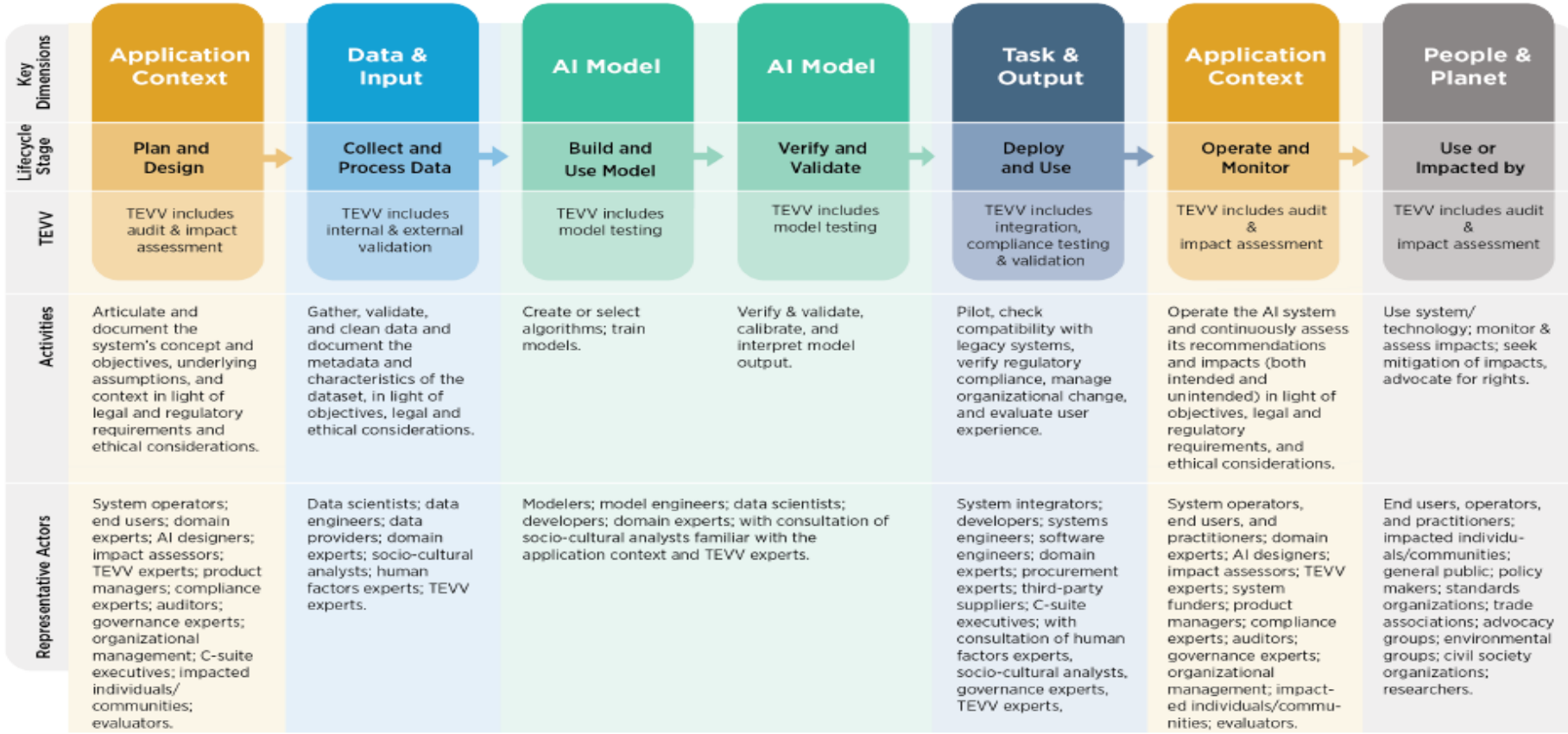
NIST, *Artificial Intelligence Risk Management Framework* (Jan. 26, 2023)

- Provides best practices for responsible development and use of AI systems
- 2 parts
  - Part 1 discusses how organizations can frame the risks related to AI and describes the intended audience
  - Part 2 comprises of the “Core” of the Framework. Describes four specific functions to help organizations address the risks of AI systems in practice
    - Govern
    - Map
    - Measure
    - Manage

NIST, *Artificial Intelligence Risk Management Framework* (Jan. 26, 2023) (cont'd)

- Framework functions to mitigate risks that may cause potential harms organized in three buckets:
  - Harms to people
  - Harms to organizations
  - Harms to ecosystems
- Each function consists of several categories and subcategories
- Govern (6 categories, 19 subcategories)
- Map (5 categories, 18 subcategories)
- Measure (4 categories, 22 subcategories)
- Manage (4 categories, 13 subcategories)

NIST, *Artificial Intelligence Risk Management Framework* (Jan. 26, 2023) (cont'd)



Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle Stage	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
TEVV	TEVV includes audit & impact assessment	TEVV includes internal & external validation	TEVV includes model testing	TEVV includes model testing	TEVV includes integration, compliance testing & validation	TEVV includes audit & impact assessment	TEVV includes audit & impact assessment
Activities	Articulate and document the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.	Gather, validate, and clean data and document the metadata and characteristics of the dataset, in light of objectives, legal and ethical considerations.	Create or select algorithms; train models.	Verify & validate, calibrate, and interpret model output.	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives, legal and regulatory requirements, and ethical considerations.	Use system/ technology; monitor & assess impacts; seek mitigation of impacts, advocate for rights.
Representative Actors	System operators; end users; domain experts; AI designers; impact assessors; TEVV experts; product managers; compliance experts; auditors; governance experts; organizational management; C-suite executives; impacted individuals/ communities; evaluators.	Data scientists; data engineers; data providers; domain experts; socio-cultural analysts; human factors experts; TEVV experts.	Modelers; model engineers; data scientists; developers; domain experts; with consultation of socio-cultural analysts familiar with the application context and TEVV experts.		System integrators; developers; systems engineers; software engineers; domain experts; procurement experts; third-party suppliers; C-suite executives; with consultation of human factors experts, socio-cultural analysts, governance experts, TEVV experts.	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impact-ed individuals/commu-nities; evaluators.	End users, operators, and practitioners; impacted individu-als/communities; general public; policy makers; standards organizations; trade associations; advocacy groups; environmental groups; civil society organizations; researchers.

Fig. 3. AI actors across AI lifecycle stages. See Appendix A for detailed descriptions of AI actor tasks, including details about testing, evaluation, verification, and validation tasks. Note that AI actors in the AI Model dimension (Figure 2) are separated as a best practice, with those building and using the models separated from those verifying and validating the models.

DHS Policy Statement 139-06 (Aug. 8, 2023)

- Implemented pursuant to Section 7224(b) of the Advancing American AI Act
- Requires DHS systems, programs, and activities using AI to conform with E.O. 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*
- Future guidance and policies on DHS use of AI will include:
  - Enterprise risk management framework approach suitable to AI
  - Develop new methods for addressing AI technologies from cyber-attacks and malicious degradation of algorithmic functions
  - DHS Information Technology Security Program will update and develop additional security requirements, as appropriate to protect AI technologies against novel cybersecurity threats and risk introduced by new applications of AI technologies
  - Formal Directive and Instructions on AI/Machine Learning 12 months from Policy

McCarter & English

Biden's E.O. 14110

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

McCarter English

What's On The Horizon?

AI.gov

- Launched in May 5, 2021
- Website dedicated to connecting the American people 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 (last updated September 1, 2023)
  - Currently more than 700 uses of AI across federal government
- Use cases offer potential development and innovation opportunities?

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

DoD AI Hierarchy of Needs

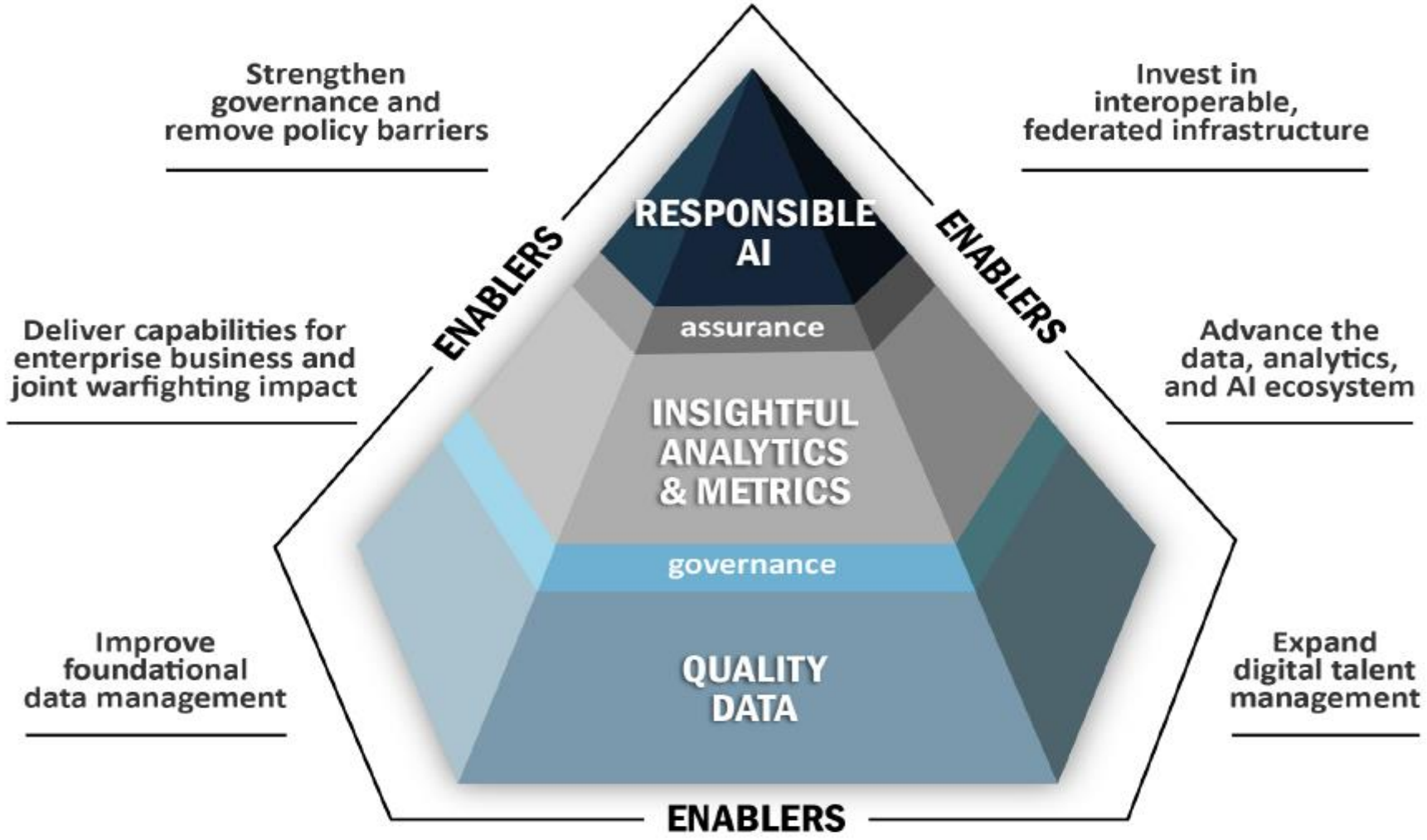


Figure 2: Strategic Goals and the AI Hierarchy of Needs

Principles Governing DoD AI Strategy

- **Improve foundational data management:** Increase quality and availability of relevant DoD data to support advanced analytics and AI capabilities
- **Deliver capabilities for enterprise business and joint warfighting impact:** Enhance and/or generate business analytics and warfighting capabilities for improved decision advantage outcomes
- **Strengthen governance and remove policy barriers:** Ensure responsible behavior, processes, and outcomes while accelerating the pace of adoption across the DoD
- **Invest in interoperable, federated infrastructure:** Optimize the DoD's federated infrastructure to support scaling and improve interoperability
- **Advance the data, analytics, and AI ecosystem:** Strengthen intergovernmental, academic, industry, and international partnerships to enable adoption
- **Expand digital talent management:** Increase hiring, training, and retention for the most critical data, analytics, and AI-related work roles

OMB, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Nov. 3, 2023)

- Proposed policy in response to AI in Government Act of 2020, Advancing American AI Act, and E.O. 14410, directing agencies to advance AI governance and innovation while managing risks from use of AI
- **Strengthening AI governance:**
  - Agencies must designate a Chief AI Officer to promote AI innovation and manage AI risk within the agency

Advancing Responsible AI Innovation

- **Advancing Responsible AI Innovation:**
  - Each CFO Act agency 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
  - Agencies should 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 ***data***sets 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

Managing Risks in Federal Procurement of AI

- Provides recommendations, with guidance forthcoming, that federal procurement of AI shall adhere to the following principles:
  - Aligning to National Values and Law
  - Transparency and Performance Improvement
  - Promoting Competition in Procurement of AI
  - Maximizing the Value of Data for AI
  - Responsibly Procuring Generative AI

Commerce Proposed Rule on Malicious Cyber-Enabled Activities and AI (Jan. 29, 2024)

- Issued in response to E.O. 13984 and E.O. 14410 regarding U.S. IaaS providers or resellers selling their products to foreign persons
- Seeks comment on the proposed Customer Identification Program ("CIP") U.S. IaaS providers are to establish and maintain, auditing CIPs, and proposes new civil and criminal penalties
- Comments open until April 29, 2024

Commerce Proposed Rule: Information Collected

- IaaS Providers allowed to develop their own risk-based CIP
- Specifies minimum customer information that needs to be collected
- Accounts opened by or on behalf of a U.S. person do not need to be verified
  - Unless a foreign beneficial owner is added to the account
- IaaS Providers must implement procedures to require foreign resellers verify the identity of a foreign purchaser of the IaaS product
- Information collected must be maintained and protected with records kept for a period of two years after date upon which the account last accessed or closed
- 1 year grace period to implement and be familiar once rule is final

Commerce Proposed Rule: IaaS Products to Train Large AI Models

- U.S. IaaS providers required to submit to Commerce when a foreign person transacts with that United States IaaS provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity
- Report on instances of training runs by foreign persons for large AI models with potential capabilities that could be used
- Reportable information includes the following identifying information about the training run:
  - Customer's name, address, the means and source of payment for the customer's account, email addresses, telephone numbers, IP addresses, and the existence of the training run

Commerce Proposed Rule: Civil and Criminal Penalties

- New civil and criminal penalties under the International Emergency Economic Powers Act rather than relying on penalty provisions under 15 CFR § 7.2001
- Intentional or knowing violations = criminal
- Unintentional = civil
- Civil penalties:
  - Up to $250,000 per person, subject to inflation, or an amount that is twice the amount of the transaction that is the basis of the violation
- Criminal Penalty
  - Up to $1 million for companies or if a natural person, imprisoned for not more than 20 years, or both
- Annual certification required

AI Contracting Opportunities

- Contracting opportunities in the following fields:
  - Deduction and reasoning systems (*e.g.*, virtual assistants)
  - Robotics and autonomous motion (*e.g.*, physical assistants)
  - Knowledge representation (*e.g.*, content curation)
  - Mixed media recognition (*e.g.*, image, sound, and sentiment)
  - Expert system (*e.g.*, synthetic media / deep fake detection)
- Opportunities at GSA:
  - Polaris (emerging technologies include AI and machine learning)
  - FASt Lane (rapid streamlining method to add new products and services onto MAS schedule contract)
- Opportunities at other Agencies
  - SEWP VI – RFP planned in 2024, several technical areas include AI/machine learning

The Open End of AI

Discussions are really just starting in earnest

- Data training sets
- Keeping pace with industry
- AI design/”AI-BOM”?
- See, e.g., *Old Dog vs. New Tricks*
- Just how much detail in what type of procurement?
- Will procurement policies lead the way in responsibly regulating AI?

McCarter English

Questions?

Bonus Tip: Don’t Be Afraid to Seek Guidance or Ask for Help!

Contact Information

Alexander W. Major, Esq.

Partner, McCarter & English LLP

www.mccarter.com
amajor@mccarter.com
O: 202-753-3440
M: 410-935-0037

Philip Lee, Esq.

Associate, McCarter & English LLP

www.mccarter.com
plee@mccarter.com
O: 202.741.8209