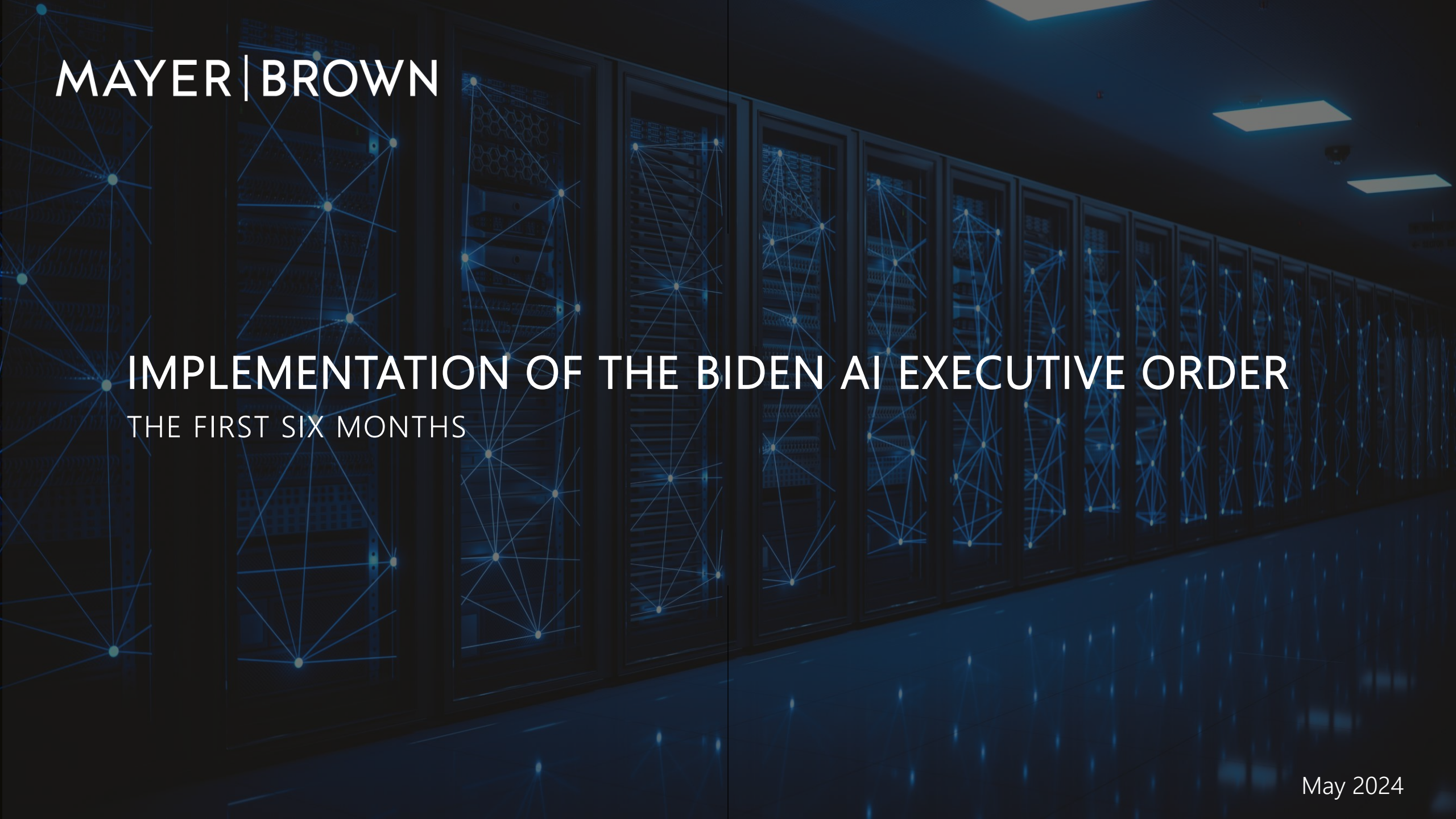


MAYER | BROWN

IMPLEMENTATION OF THE BIDEN AI EXECUTIVE ORDER

THE FIRST SIX MONTHS

May 2024

PRESENTING TODAY

Stephen Lilley

Stephen is a partner in the Washington DC office of Mayer Brown. A member of the firm's Cybersecurity & Data Privacy, National Security, and Litigation practices, Stephen develops strategies to navigate cutting-edge and interrelated litigation, regulatory, and policy challenges rooted in data and technology. He has been named a "Leading Lawyer" for Cyber Law by the Legal 500. Stephen works with clients on complex challenges presented by Artificial Intelligence, including on the development of governance programs for AI, managing the security risks associated with the implementation of AI, and AI policy matters.

Howard Waltzman

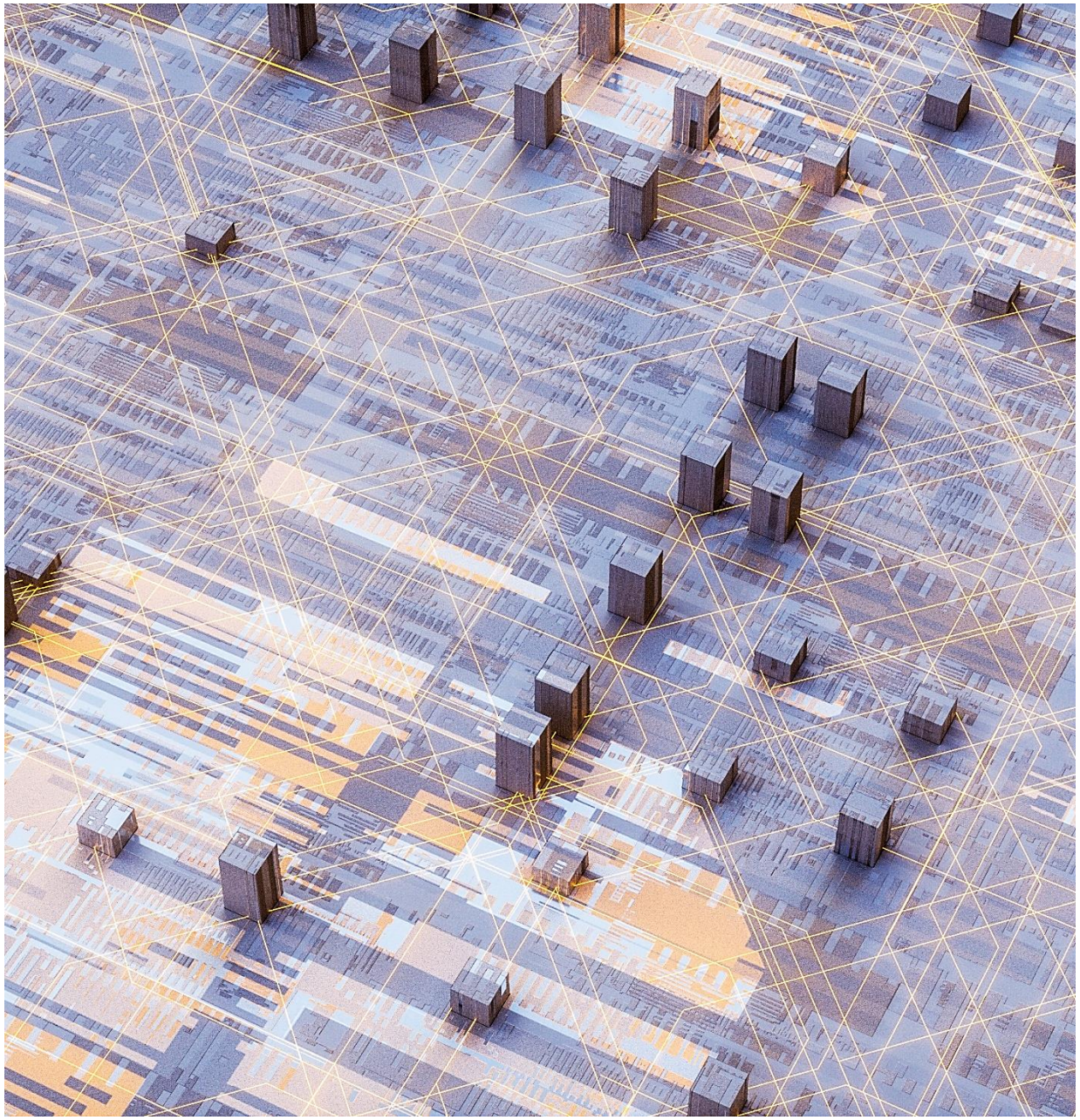
Howard advises some of the nation's leading service providers, manufacturers and trade associations in regulatory, compliance and legislative matters, including with respect to artificial intelligence, cybersecurity, privacy, communications services and other complex public policy issues involving technology. Howard drafts regulatory pleadings and license applications; legislation, Congressional testimony and legislative history; and compliance programs. He appears personally before Members of Congress, Cabinet department officials, key Congressional, Administration, agency staff, and has testified personally at legislative hearings.

Sasha Keck

Sasha is a senior associate in the firm's Cybersecurity & Data Privacy and Litigation & Dispute Resolution practices, focusing her practice on complex and cutting-edge legal issues related to cybersecurity and data privacy. Her practice includes counseling on compliance with global privacy and security frameworks, cyber incident response, and crisis management. Sasha also has experience advising US and multinational companies on conducting internal investigations and responding to government inquiries, including those from state attorneys general, the Department of Health and Human Services, and the Department of Justice.

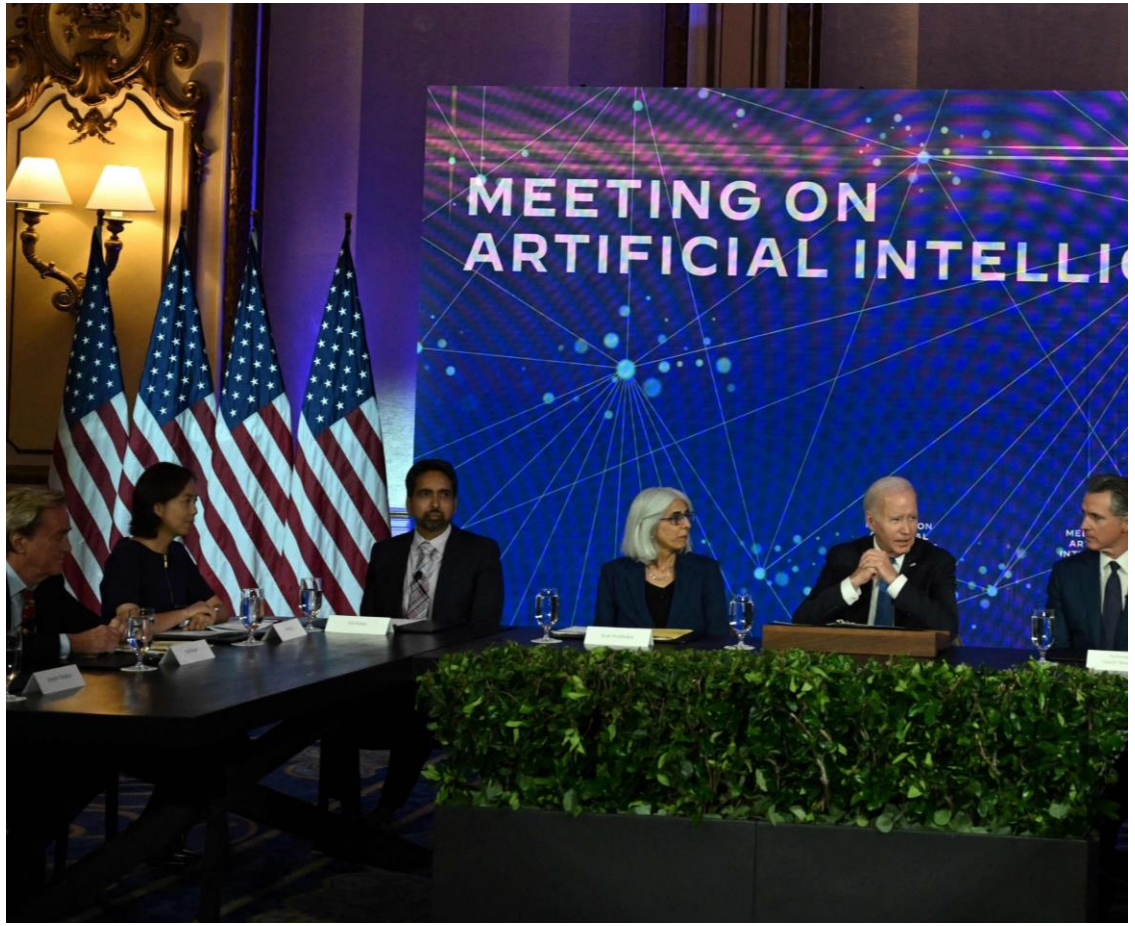
AGENDA

- AI Executive Order Overview
- Recent Developments
  - Office of Management & Budget Issues AI Memorandum to Federal Agencies
  - Required Reporting re. Dual-Use Foundation Models
  - Treasury Report on Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector
  - Proposed Rule Requiring IaaS Providers to Verify Identities of Foreign Customers
  - NIST Guidance on AI Risk Management
  - DHS Guidance on AI and Critical Infrastructure
- Other Key Actions Ahead



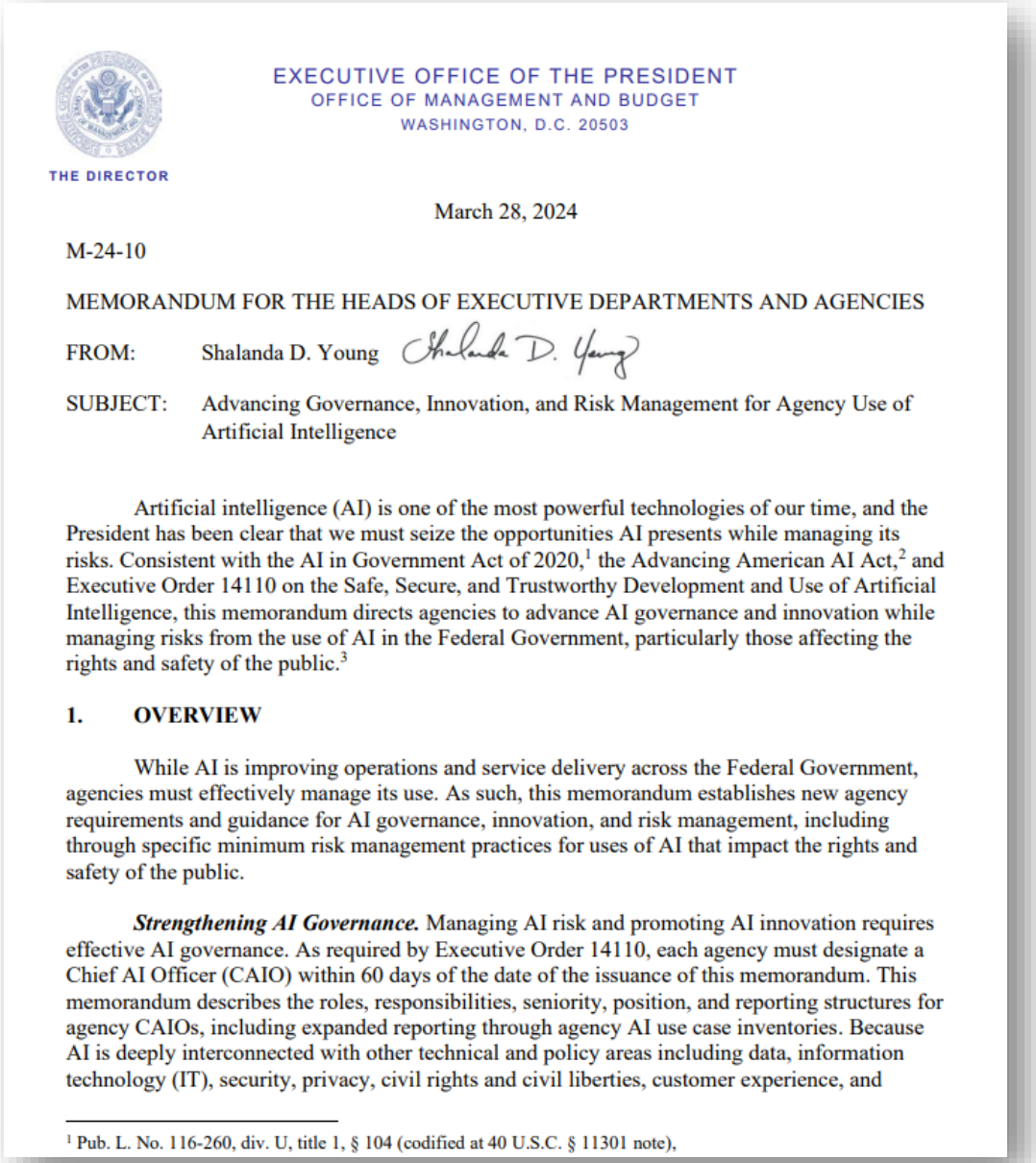
EXECUTIVE ORDER ON THE SAFE, SECURE, AND TRUSTWORTHY DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE (OCT 2023)

- In October 2023, President Biden launched sweeping action across the executive branch pursuant to his Executive Order on Artificial Intelligence.
- The EO reflects an all-tools approach to try to encourage AI innovation while also addressing the wide range of risks presented by AI (e.g., privacy, security, and civil rights).
- While the EO focuses on establishing guardrails for development and implementation of AI in the private sector, the EO also directs the federal government to widely consider the deployment of AI for government functions.
- The EO leverages authorities from the International Emergency Economic Powers Act (IEEPA) and the Defense Production Act (DPA), however the limited authorities and appropriations of executive branch agencies tasked with implementing the EO likely means that congressional action will be needed.



OFFICE OF MANAGEMENT & BUDGET ISSUES AI MEMORANDUM TO FEDERAL AGENCIES

- On March 28, 2024, OMB Director Young issued a memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.
- Applies to "new and existing AI that is developed, used, or procured by or on behalf of covered agencies."
- Key Requirements:
  - Designate a Chief AI Officer to coordinate use of AI, promote AI innovation, and manage risks.
  - Submit an inventory of AI uses cases that are safety-impacting and rights-impacting.
  - Develop and publicly release an AI strategy outlining current and planned uses of AI, governance processes, workforce capacity, etc.
  - Ensure adequacy of IT infrastructure, data management capacity, and cybersecurity.
  - Assess potential beneficial uses and establish adequate safeguards for generative AI.
  - Share custom-developed code with other agencies and maintain it as open source.
  - Adhere to minimum risk management practices for safety-impacting and rights-impacting AI.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

March 28, 2024

M-24-10

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young

SUBJECT: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

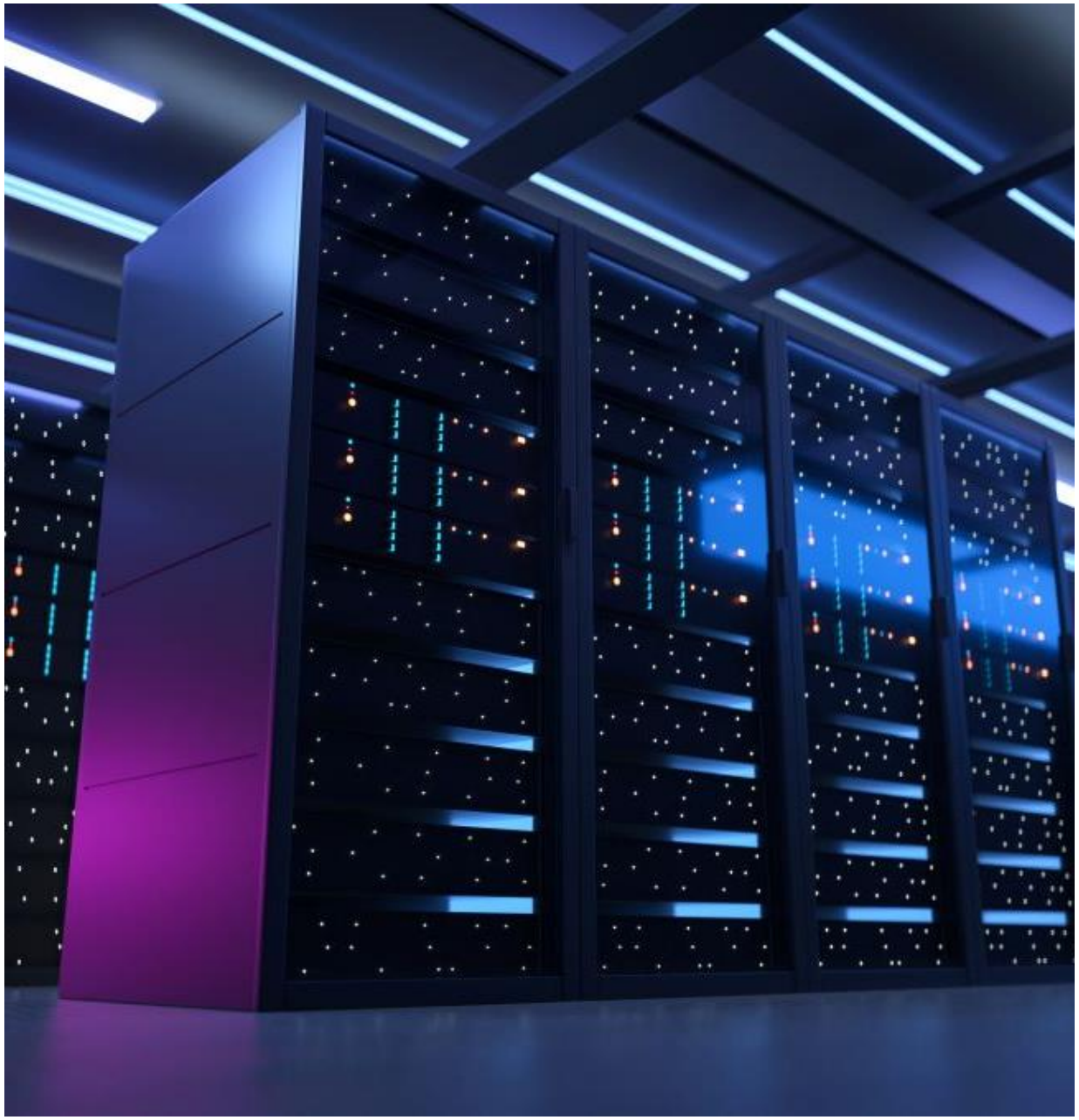
Artificial intelligence (AI) is one of the most powerful technologies of our time, and the President has been clear that we must seize the opportunities AI presents while managing its risks. Consistent with the AI in Government Act of 2020,[1] the Advancing American AI Act,[2] and Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, this memorandum directs agencies to advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public.[3]

1. OVERVIEW

While AI is improving operations and service delivery across the Federal Government, agencies must effectively manage its use. As such, this memorandum establishes new agency requirements and guidance for AI governance, innovation, and risk management, including through specific minimum risk management practices for uses of AI that impact the rights and safety of the public.

Strengthening AI Governance. Managing AI risk and promoting AI innovation requires effective AI governance. As required by Executive Order 14110, each agency must designate a Chief AI Officer (CAIO) within 60 days of the date of the issuance of this memorandum. This memorandum describes the roles, responsibilities, seniority, position, and reporting structures for agency CAIOs, including expanded reporting through agency AI use case inventories. Because AI is deeply interconnected with other technical and policy areas including data, information technology (IT), security, privacy, civil rights and civil liberties, customer experience, and

[1] Pub. L. No. 116-260, div. U, title 1, § 104 (codified at 40 U.S.C. § 11301 note),



DEPARTMENT OF COMMERCE STARTS REQUIRING REPORTING REGARDING DUAL-USE FOUNDATION MODELS

- The requirement marks the first formalized safety and security information-sharing program between some of the largest AI developers and the federal government.
- The Department of Commerce is authorizing such data collection under the Defense Production Act. While lawmakers and industry groups have pushed back on such authority, the Biden Administration has announced that it has implemented this aspect of the EO.
- Under the EO, the required reporting includes:
  - "Ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats"
  - "The ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights."
  - "The results of any developed dual-use foundation model's performance in relevant AI red-team testing…"

DEPARTMENT OF THE TREASURY RELEASES REPORT ON ARTIFICIAL INTELLIGENCE-SPECIFIC CYBERSECURITY RISKS IN THE FINANCIAL SECTOR

- The report is based on interviews with several financial institutions across the United States on their use of AI in the areas of cybersecurity and fraud detection.
- Key Findings:
  - Firms have used AI systems for years, particularly for fraud detection.
  - Firms are taking a cautious and risk-based approach to the adoption of generative AI.
  - Larger firms are employing hundreds of AI developers to develop in-house solutions based on proprietary solutions.
  - Firms are concerned about the use of AI by threat actors to lower barriers to cyber attacks and to create synthetic identities that can evade fraud detection tools.
- Best Practices:
  - Integrate AI into existing enterprise risk management programs.
  - Map the data supply chain.
  - Apply cybersecurity best practices and security controls to AI systems.

BIS/COMMERCE DEPARTMENT PROPOSED RULE REQUIRING IAAS PROVIDERS TO VERIFY IDENTITIES OF FOREIGN CUSTOMERS

- The Notice of Proposed Rulemaking (NPRM) results from President's Trump's EO requiring Infrastructure as a Service (IaaS) providers to establish identity verification procedures for foreign customers and President Biden's AI EO requiring foreign resellers of IaaS products to institute the same procedures and requiring verification and reporting for AI training runs conducted by foreign customers.
- The proposed rule covers a broad range of IaaS product offerings inclusive of managed and unmanaged products and services and virtualized products and services.
- Key Provisions:
  - IaaS providers would have to implement a Customer Identification Program (CIP) to collect customer information and verify their customers' identities.
  - The Secretary of Commerce would have the power to prohibit or impose conditions on opening or maintaining accounts with any IaaS provider by a foreign person.
- Industry representatives submitted a range of comments before the comment period ended on April 29th and broadly pushed back on the proposal.

NIST DRAFT GUIDANCE ON AI RISK MANAGEMENT

- On April 29, 2024, the Commerce Department announced NIST's release of four draft documents in further implementation of the Executive Order, with comments due by June 2, 2024:
  - The *AI RMF Generative AI Profile* is intended to help organizations identify and manage unique risks posed by generative AI.
  - *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* seeks to help address concerns around malicious training data adversely affecting generative AI systems. It also offers guidance on the training data and data collection process.
  - *Reducing Risks Posed by Synthetic Content* discusses methods for detecting, authenticating and labeling synthetic content, including digital watermarking and metadata recording. It is intended to reduce risks from synthetic content through relevant technical approaches.
  - *A Plan for Global Engagement on AI Standards* is designed to drive the worldwide development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing.
- NIST also announced a new program called NIST GenAI that it will use to evaluate and measure generative AI technologies. The program will inform the work of the U.S. AI Safety Institute at NIST.


NIST AI 600-1

NIST Special Publication 800
NIST SP 800-218A ipd

Secure Software Development Practices for Generative AI and Dual-Use Foundation Models

An SSDF Community Profile

Initial Public Draft

Harold Booth
Murugiah Souppaya
Apostol Vassilev
Computer Security Division
Information Technology Laboratory

Martin Stanley
Cybersecurity and Infrastructure Security Agency (CISA)

Michael Ogata
Applied Cybersecurity Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-218A.ipd

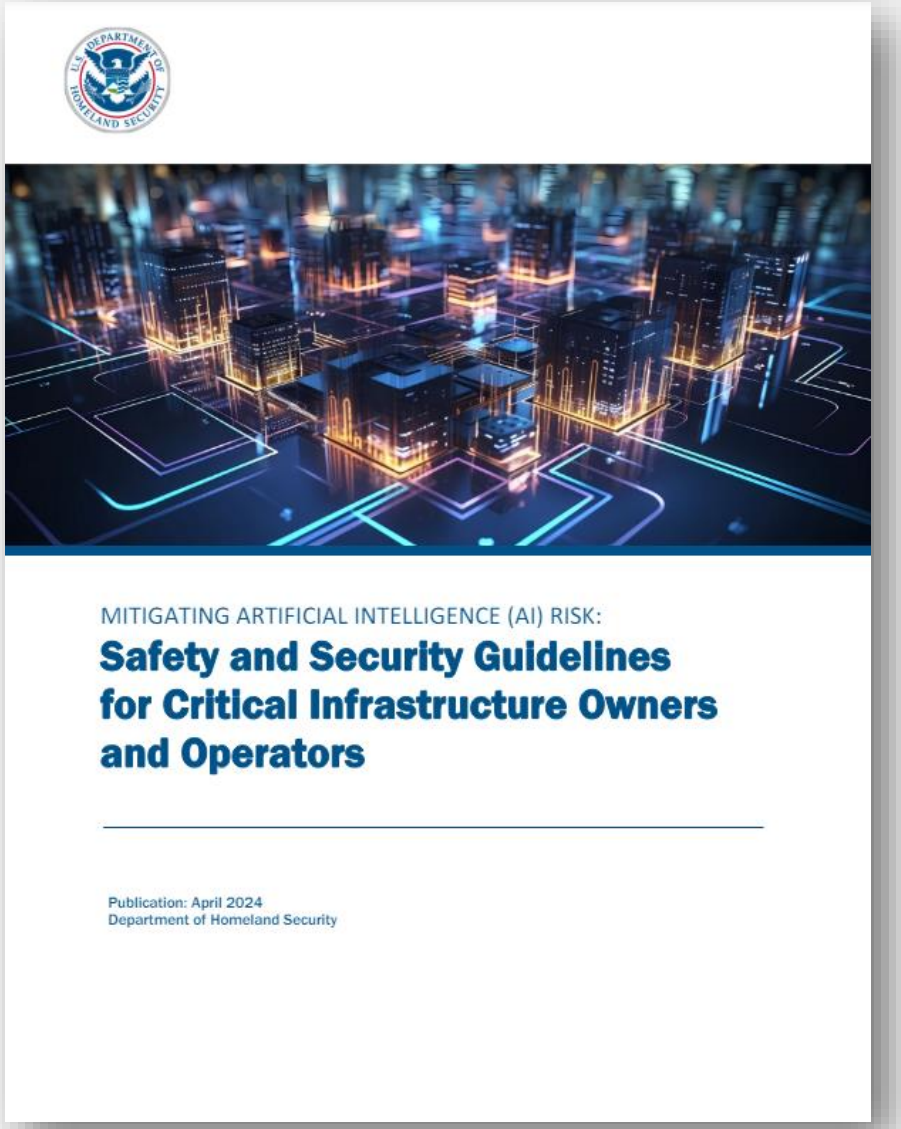
April 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

DHS GUIDELINES AND REPORT TO SECURE CRITICAL INFRASTRUCTURE AND WEAPONS OF MASS DESTRUCTION FROM AI-RELATED THREATS

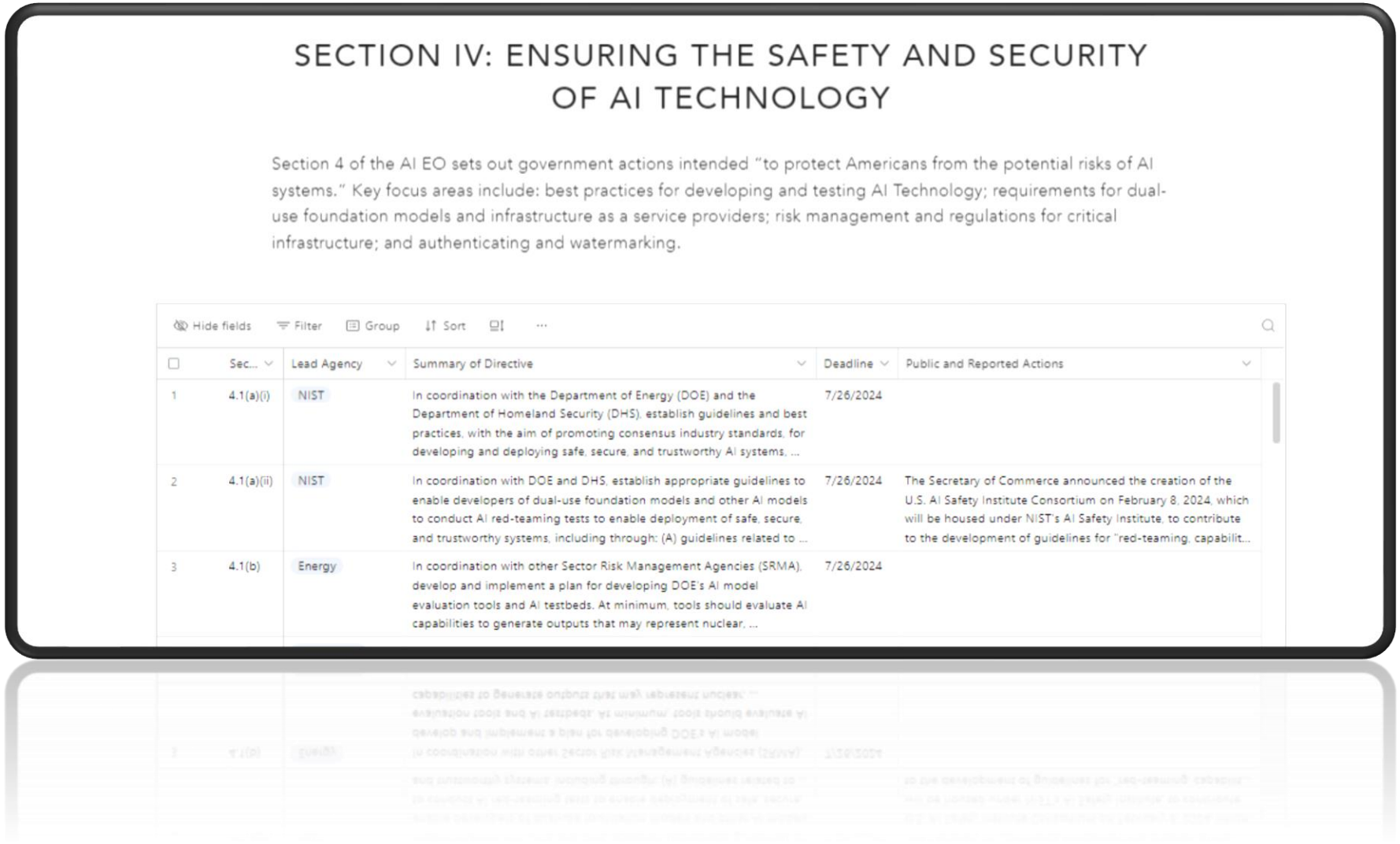
- On April 26, 2024, DHS released its report *Mitigating Artificial Intelligence (AI) Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators*.
- DHS collaborated with a wide range of agencies in developing these guidelines, including the Department of Commerce, the Sector Risk Management Agencies (SRMAs) for the 16 critical infrastructure sectors, and relevant independent regulatory agencies.
- The guidelines incorporate the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), including its four functions that help organizations address the risks of AI systems: Govern, Map, Measure, and Manage.
- The guidelines are written to apply to all critical infrastructure sectors, although DHS encourages owners and operators of critical infrastructure to consider sector-specific and context-specific AI risks and mitigations.



LOOKING AHEAD

- Further implementation of the AI Executive Order across each focus area, to include:
  - Consideration of potential changes to the Federal Acquisition Regulation
  - Efforts to implement DHS guidance through regulation
- Legislative activity at the state and federal level
- Potential implications of the 2024 election

PLEASE CHECK THE MAYER BROWN AI EO ACTION TRACKER FOR FURTHER UPDATES



SECTION IV: ENSURING THE SAFETY AND SECURITY OF AI TECHNOLOGY

Section 4 of the AI EO sets out government actions intended "to protect Americans from the potential risks of AI systems." Key focus areas include: best practices for developing and testing AI Technology; requirements for dual-use foundation models and infrastructure as a service providers; risk management and regulations for critical infrastructure; and authenticating and watermarking.

Hide fields | Filter | Group | Sort | ...

	Sec...	Lead Agency	Summary of Directive	Deadline	Public and Reported Actions
1	4.1(a)(i)	NIST	In coordination with the Department of Energy (DOE) and the Department of Homeland Security (DHS), establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, ...	7/26/2024	
2	4.1(a)(ii)	NIST	In coordination with DOE and DHS, establish appropriate guidelines to enable developers of dual-use foundation models and other AI models to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems, including through: (A) guidelines related to ...	7/26/2024	The Secretary of Commerce announced the creation of the U.S. AI Safety Institute Consortium on February 8, 2024, which will be housed under NIST's AI Safety Institute, to contribute to the development of guidelines for "red-teaming, capabilit...
3	4.1(b)	Energy	In coordination with other Sector Risk Management Agencies (SRMA), develop and implement a plan for developing DOE's AI model evaluation tools and AI testbeds. At minimum, tools should evaluate AI capabilities to generate outputs that may represent nuclear, ...	7/26/2024	

Visit the AI EO Implementation Tracker here

MAYER | BROWN