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

THE DIRECTOR

April 3, 2025

M-25-21

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust

OVERVIEW

On January 23, 2025, President Trump signed Executive Order (E.O.) 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, to advance the United States' global AI dominance and to promote responsible AI innovation. Now more than ever, agencies[1] are empowered to drive AI innovation and seize the opportunity to apply the best of American AI. Through this memorandum, agencies are directed to provide improved services to the public, while maintaining strong safeguards for civil rights, civil liberties, and privacy. This memorandum provides guidance to agencies on ways to promote human flourishing, economic competitiveness and national security. Agencies must follow the detailed implementation instructions and requirements included in the Appendix. This memorandum rescinds and replaces Office of Management and Budget (OMB) Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*.

SCOPE

This memorandum is directed to the heads of all Executive Branch departments and agencies, including independent regulatory agencies.[2]

GUIDANCE ON FEDERAL USE OF AI

The United States is at the forefront of AI development, and agencies must adopt a forward-leaning and pro-innovation approach that takes advantage of this technology to help shape the future of government operations. Agencies are encouraged to harness solutions that bring the best value to taxpayers, increase quality of public services, and enhance government efficiency. Through this memorandum, agencies will be charged to lessen the burden of bureaucratic restrictions and to build effective policies and processes for the timely deployment

[1] The term "agency" has the meaning provided in 44 U.S.C. § 3502(1).
[2] The term "independent regulatory agency" is defined in 44 U.S.C. § 3502(5).

Marvell Semiconductor, Inc. - Ex. 1046, Page 000001
IPR2025-01218 (Marvell Semiconductor, Inc. v. Credo Technology Group Ltd.)

of AI. Agencies are directed to accelerate the Federal use of AI by focusing on three key priorities: innovation, governance, and public trust.[3] Consistent with these goals, agencies must undertake the requirements described in the Appendix. This includes the following:

Agencies must remove barriers to innovation and provide the best value for the taxpayer.

Agencies must lean forward on adopting effective, mission-enabling AI to benefit the American people. To best achieve this, agencies must remove unnecessary and bureaucratic requirements that inhibit innovation and responsible adoption. Agencies must develop public AI strategies that elevate AI adoption and innovation as a priority, while increasing transparency to the American public, civil society, and industry.

Agencies must maximize the value of existing investments to ensure speedy deployment and to protect taxpayer dollars from duplicative spending, including sharing resources within an agency and across government. Agencies must also reuse resources that enable AI adoption, such as agency data, models, code, and assessments of AI performance. When choosing to pursue an AI acquisition, agencies should invest in the American AI marketplace and maximize the use of AI products and services that are developed and produced in the United States. To lead these innovation priorities, agencies are encouraged to develop and retain AI and AI-enabling talent who have the technical experience to scale and govern AI to improve mission outcomes.

Agencies must empower AI leaders to accelerate responsible AI adoption.

Agencies must cut down on bureaucratic bottlenecks and redefine AI governance as an enabler of effective and safe innovation. As a step towards accelerating responsible adoption, agencies must establish clear expectations for their workforce on appropriate AI use—particularly when an agency is using AI to support consequential decision-making. Agency policies must enable agency heads to delegate responsibilities and accountability for risk acceptance to appropriate officials throughout the agency, ensuring that swift action is possible with sufficient guardrails in place.

Agencies must identify a Chief AI Officer to champion their agency's AI goals by advising on how to make these improvements, and agencies must allocate appropriate resources and responsibilities to effect the changes in this memorandum. To support these efforts, OMB will convene and chair an interagency council to maximize agency efficiencies by coordinating the development and use of AI in their programs and operations. Agencies must also be accountable to the taxpayer and must continue with all relevant reporting requirements, including updating their annual AI use case inventory, compliance plans, and reporting as requested by OMB.

Agencies must ensure their use of AI works for the American people.

Every day, the Federal Government takes action and makes decisions that have consequential impacts on the public. If AI is used to perform such action, agencies must deploy

[3] The requirements in this section are consistent with the following laws and policies: AI in Government Act of 2020, Advancing American AI Act, E.O. 13960, and E.O. 14179.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000002

trustworthy AI, ensuring that rapid AI innovation is not achieved at the expense of the American people or any violations of their trust.

As such, agencies are directed to implement minimum risk management practices for AI that could have significant impacts when deployed ("high-impact AI"), as outlined in the Appendix, and to prioritize the use of AI that is safe, secure, and resilient. When the high-impact AI is not performing at an appropriate level, agencies must have a plan to discontinue its use until actions are taken to achieve compliance with this memorandum. If proper risk mitigation is not possible, agencies must cease the use of the AI. In an effort to reduce redundancy and unnecessary burden, agencies are reminded that risk management practices for AI should be proportionate to the anticipated risk from its intended use. These protections will ensure that agencies are serving the American public.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000003

Appendix: M-25-21 Implementation Guidance for Agencies

1. SCOPE

This memorandum provides guidance to agencies on how to innovate and promote the responsible adoption, use, and continued development of AI, while ensuring appropriate safeguards are in place to protect privacy, civil rights, and civil liberties, and to mitigate any unlawful discrimination, consistent with the AI in Government Act.[4] This memorandum does not address general issues related to Federal information and information systems. This memorandum does not supersede, and should be considered in concert with, other more general Federal policies.

Agencies must continue to comply with applicable law and OMB policies in other domains relevant to AI, and must continue to coordinate compliance across the agency with all appropriate officials. All agency officials retain their existing authorities and responsibilities established in other laws and policies.

a. Covered Agencies. Except as specifically noted, this memorandum applies to all agencies defined in 44 U.S.C. § 3502(1).[5] As noted in the relevant sections, some requirements in this memorandum apply only to Chief Financial Officers Act (CFO Act) agencies as identified in 31 U.S.C. § 901(b), and other requirements do not apply to elements of the Intelligence Community, as defined in 50 U.S.C. § 3003.

b. Covered AI. This memorandum provides requirements and recommendations that apply to new and existing AI that is developed, used, or acquired by or on behalf of covered agencies. This memorandum does not, by contrast, govern agencies':

---

[4] Consistent with provisions of the AI in Government Act of 2020, which required the issuance of this memorandum, and the Advancing American AI Act, this memorandum sets forth multiple independent requirements and recommendations for agencies, and OMB intends that these requirements and recommendations be treated as severable. For example, the memorandum's provisions regarding the integrating of AI governance in Section 3 are capable of operating independently, and serve an independent purpose, from the required risk management practices set forth in Section 4. Likewise, each of Section 4's individual risk management practices serve an independent purpose and can function independently from the other risk management practices. Accordingly, while this memorandum governs only agencies' own use of AI and does not create rights or obligations for the public, in the event that a court were to stay or enjoin application of a particular provision of this memorandum, or its application to a particular factual circumstance, OMB would intend that the remainder of the memorandum remain operative.

[5] The term "agency," as used in both the AI in Government Act of 2020 and the Advancing American AI Act, is defined as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency," but does not include the Government Accountability Office; the Federal Election Commission; the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. 44 U.S.C. § 3502(1); see AI in Government Act of 2020 § 102(2) (defining "agency" by reference to § 3502); Advancing American AI Act § 7223(1) (same). As a result, independent regulatory agencies as defined in 44 U.S.C. § 3502(5), which were not included in the definitions of "agency" in Executive Order 13960, are covered by this memorandum.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000004

i. regulatory actions designed to prescribe law or policy regarding non-agency uses of AI; [6]
ii. assessments of particular AI applications because the AI provider is the target or potential target of a regulatory enforcement, law enforcement, or national security action;[7]
iii. development of metrics, methods, and standards to test and measure AI, where such metrics, methods, and standards result in use by the general public or the government as a whole; or
iv. use of AI to carry out basic research or applied research, except where the purpose of such research is to develop particular AI applications for agency use.

The requirements and recommendations of this memorandum apply to system functionality that implements or is reliant on AI, rather than to the entirety of an information system that incorporates AI. As noted in the relevant sections, some requirements in this memorandum apply only in specific circumstances in which agencies use AI that is deemed high-impact.

c. Applicability to National Security Systems. This memorandum does not cover AI when it is being used as a component of a National Security System.[8]

2. DRIVING AI INNOVATION

The Federal Government has demonstrated that AI can improve public services, increase mission effectiveness, and reduce costs to the American people. Agencies have a responsibility to identify and remove barriers to further responsible AI adoption and application, where practicable, while providing meaningful public transparency into the Federal Government's use of AI. Agencies should focus on improving mission effectiveness through the use of AI by building upon their existing capabilities to drive responsible AI innovation, strengthen their AI and AI-enabling talent, and improve their ability to develop and procure AI.

a. Developing Agency AI Strategies

Within 180 days of the issuance of this memorandum, each CFO Act agency must develop an AI Strategy for identifying and removing barriers to their responsible use of AI and for achieving enterprise-wide improvements in the maturity of their applications. Agencies must use the AI Strategies template, to be provided by OMB, and make their AI Strategies publicly

---

[6] For guidance on regulatory and non-regulatory approaches to AI applications developed and deployed outside of the Federal government and best practices to reduce barriers to the development and adoption of AI technologies, agencies should consult OMB Memorandum M-21-06, *Guidance for Regulation of Artificial Intelligence Applications* (Nov. 17, 2020), https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/11/M-21-06.pdf.
[7] AI is not in scope when it is the target or potential target of such an action, but it is in scope when the AI is used to carry out an enforcement action. For example, when evaluating an AI tool to determine whether it violates the law, the AI would not be in scope; if an agency was using that same AI tool to assess a different target, then the AI would be in scope.
[8] AI innovation and risk for National Security Systems must be managed appropriately, but these systems are governed through other policy. Agencies should reference existing guidelines in place, such as the Department of Defense's (DoD) *Responsible Artificial Intelligence Strategy and Implementation Pathway* and the Office of the Director of National Intelligence's *Principles of Artificial Intelligence Ethics for the Intelligence Community*, as well as policies governing specific high-risk national security applications of AI, such as DoD Directive 3000.09, *Autonomy in Weapon Systems,* https://ogc.osd.mil/Portals/99/autonomy_in_weapon_systems_dodd_3000_09.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000005

available on the agency's website. To ensure accountability to the taxpayer, strategies should be understandable, accessible to the public, and transparent about how their investments in AI innovation benefit the American people.

Agencies should assess their AI maturity goals and accelerate and scale AI adoption, by appropriately resourcing areas such as data governance, information technology (IT), infrastructure, quality data assets, integration and interoperability, accessibility, privacy, confidentiality, and security. Agencies must strive to utilize and scale existing tools, processes, and resources for AI governance whenever possible to avoid the creation of additional bureaucracy, and invest in technical solutions to make compliance more efficient. Agency AI Strategies must be consistent with this memorandum and include:

i. current and planned AI use cases that are most impactful to an agency's mission, operations, or service delivery;[9]

ii. an assessment of the agency's current state of AI maturity and a plan to achieve the agency's AI maturity goals, by addressing, at a minimum, plans or processes to:

   A. develop AI-enabling infrastructure[10] across the AI lifecycle including development, testing, deployment, continuous monitoring;[11]
   B. ensure access to quality data[12] for AI and data traceability;[13]
   C. develop enterprise capacity for AI innovation;
   D. provide AI tools and capacity to support the agency's AI research and development (R&D) efforts;
   E. develop the necessary operations, governance, and infrastructure to manage risks from the use of AI, including risks related to information security and privacy;
   F. recruit, hire, train, retain, and empower an AI-ready workforce and achieve AI literacy for non-practitioners involved in AI; and
   G. identify, track, and facilitate future AI investment or procurement.

---

[9] Consistent with sections 7225(d) and 7228 of the Advancing American AI Act, this requirement applies to CFO Act agencies except for the Department of Defense, and does not apply to elements of the Intelligence Community, as defined in 50 U.S.C. § 3003(4). Information that would be protected from release if requested under 5 U.S.C. § 552 need not be included in the strategy.

[10] Agencies should ensure that their AI projects have access to adequate IT infrastructure, including high-performance computing infrastructure specialized for AI training and inference, where necessary. Agencies should also ensure adequate access for AI developers to the software tools, open-source libraries, and deployment and monitoring capabilities necessary to rapidly develop, test, and maintain AI applications.

[11] Agencies should update, as necessary, processes for information system authorization and continuous monitoring to better address the needs of AI applications.

[12] Agencies should develop adequate infrastructure and capacity to sufficiently share, curate, and govern agency data for use in training, testing, and operating AI. This includes an agency's capacity to maximize appropriate access to and sharing of both internally held data and agency data managed by third parties. Agencies should also explore the possible utility of and legal authorities supporting the use of publicly available information, and encourage its use where appropriate and consistent with the data practices outlined in this memorandum.

[13] In this context, traceability refers to an agency's ability to track and internally audit datasets used for AI, and where relevant, key metadata. A significant enabler of traceability is clear documentation that is meaningful or understandable to individual users and reflects the process for model-driven development.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000006

b. Sharing of Agency Data and AI Assets

Agencies can save taxpayer dollars by actively engaging in quality data governance and management and the reuse of data and AI assets. Chief AI Officers (CAIOs), as described in Section 3(a)(i), and Chief Data Officers (CDOs) are encouraged to coordinate internally and across the Federal Government on criteria for data interoperability and standardization of data formats as a means of increased AI adoption. Agencies should identify and share commonly used packages or functions that have the greatest potential for reuse by other agencies or by the public.

i. Encouraging Reuse of AI Code and Models. Agencies must proactively share across the Federal Government their custom-developed code—including models and model weights—whether agency developed or procured, for AI applications in active use, except in the circumstances described in paragraphs A through D below. Agencies must also prioritize sharing AI code, models, and data government-wide, consistent with the Open, Public, Electronic and Necessary (OPEN) Government Data Act.[14] Agencies, where practicable, must also release and maintain AI code as open source software in a public repository[15] unless the:

   A. sharing of the code is restricted by law or regulation, including patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulations, or Federal laws and regulations governing classified information;
   B. sharing of the code would create an identifiable risk to national security, confidentiality of Government information, individual privacy, or the rights or safety of the public;
   C. agency is prevented from doing so by a contractual obligation; or
   D. sharing of the code would create an identifiable risk to agency mission, programs, or operations, or to the stability, security, or integrity of an agency's systems or personnel.

ii. Sharing and Releasing AI Data Assets. Data used to develop and test AI may constitute a "data asset" within the meaning of 44 U.S.C. § 3502(17). Agencies must include them in their comprehensive data inventories if required by the OPEN Government Data Act and OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-*

[14] Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, https://www.congress.gov/115/statute/STATUTE-132/STATUTE-132-Pg5529.pdf.

[15] For guidance and best practices related to sharing code and releasing it as open source, agencies should consult OMB Memorandum M-16-21, *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (Aug. 8, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_21.pdf. Agencies are additionally encouraged to draw upon existing collaboration methods to facilitate the sharing and release of code and models, the General Services Administration's AI Community of Practice, and https://www.code.gov, as well as other publicly available code repositories.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000007

Based Policymaking Act of 2018: Open Government Data Access and Management Guidance.[16]

iii. Unintended Disclosure of Data from AI Models. Consistent with Section 2(d)(i), agencies should assess the risks associated with AI models, as they may reveal sensitive details of the data used to develop them.[17]

c. Leveraging American AI and Innovation

Executive Order 14179 recognizes the importance of American AI development to promote human flourishing, economic competitiveness, and national security. Consistent with applicable law, it is the policy of the United States to buy American and to maximize the use of AI products and services that are developed and produced in the United States. OMB Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government,* covers the importance of American AI in federal procurement.

d. Effective Federal Procurement of AI

This section provides agencies with recommendations for the responsible procurement of AI capabilities to facilitate compliance with the minimum risk management practices for high-impact AI use cases detailed in Section 4. Consistent with Section 7224(d) of the Advancing American AI Act and Executive Order 14179, OMB will issue revised guidance to ensure that Federal contracts for the acquisition of an AI product or service align with the recommendations of this memorandum.

i. Maximizing the Value of Data for AI. In contracts for AI products and services, agencies should treat relevant data, or improvements to that data—such as cleaning and labeling—as a critical asset for their AI maturity. Agencies should take steps to ensure that their contracts retain sufficient rights to Federal Government data and retain any improvements to that data, including the continued design, development, testing, and operation of AI. Additionally, agencies should consider contractual terms that prevent vendor lock-in and also protect Federal information used by vendors in the development and operation of AI products and services for the Federal Government. Contract terms should protect such data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from the agency.

ii. Performance Improvement. Agencies, where practicable, are encouraged to better track and evaluate performance of their procured AI by:

[16] Where such data is already publicly available, agencies are not required to duplicate it, but should maintain and share the provenance of such data and how others can access it. For guidance on the sharing and release of data assets, see OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance* (Jan. 15, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/01/M-25-05-Phase-2-Implementation-of-the-Foundations-for-Evidence-Based-Policymaking-Act-of-2018-Open-Government-Data-Access-and-Management-Guidance.pdf.

[17] The risks of unintended disclosure differ by model, and agencies should also not assume that an AI model poses the same privacy and confidentiality risks as the data used to develop it.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000008

A. documenting known capabilities and limitations of the AI and any guidelines on how the system is intended to be used;
B. documenting provenance of the data used to train, fine-tune, or operate the AI;
C. conducting ongoing testing and validation on AI model performance; the effectiveness of vendor AI offerings; and associated risk management measures, including by testing in real-world conditions;
D. assessing for overfitting to known test data, ensuring that AI developers or vendors are not directly relying on the test data to train their AI systems;[18]
E. considering contractual terms that prioritize the continuous improvement, performance monitoring, and evaluation of effectiveness of procured AI; and
F. requiring sufficient post-award monitoring and evaluation of effectiveness of the AI, where appropriate in the context of the product or service acquired.

iii. Promoting Competition in Federal Procurement of AI. Agencies should adopt procurement practices that encourage competition to sustain a robust Federal AI marketplace, such as by preferencing interoperable AI products and services.

e. Enabling an AI-Ready Federal Workforce

Training the Federal workforce about AI improves efficiency and increases AI adoption. The Federal workforce has a responsibility to develop and maintain, at a minimum, foundational knowledge of how to use AI responsibly in performing their official duties. Agencies are strongly encouraged to prioritize recruiting, developing, and retaining technical talent in AI roles. The benefits include increasing enterprise capacity for responsible AI innovation, providing the Federal workforce pathways to AI up-skilling, and assisting employees in applying AI to their work. Agencies should take action by:

i. Leveraging AI Trainings and Resources to Upskill Existing Staff. Agencies should leverage AI training programs and resources, such as the annual training made available government-wide by OMB and GSA,[19] to strengthen the technical skills of staff in AI and AI-enabling roles. Agencies should develop additional technical training or resources as needed to increase practical, hands-on expertise with AI technologies.

ii. Promoting AI Talent. Agencies should focus recruitment efforts on individuals that have demonstrated operational experience in designing, deploying, and scaling AI systems in high-impact environments.

iii. Ensuring Accountability. Agencies, in coordination with relevant agency officials, should identify and track, as appropriate, existing and emerging needs related to AI talent and expertise across the agency to ensure technical talent and resources are allocated properly and aligned with mission needs.

---

[18] For instance, using validation data to train a model could lead the model to learn spurious correlations that make the model appear accurate in tests but degrade the real-world performance of the AI system.
[19] *See* the AI Training Act, Pub. L. No. 117-207, https://www.congress.gov/117/plaws/publ207/PLAW-117publ207.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000009

3. IMPROVING AI GOVERNANCE

Effective AI governance is key to accelerated innovation as it empowers professionals at all levels to align processes, establish clear policies, and foster accountability while reducing unnecessary barriers to AI adoption. To that end, agencies must identify key officials to lead agency AI adoption and promote the sharing of best practices, empowering the entire Federal workforce to leverage AI in fulfilling their mission. Consistent with these goals, agencies must undertake the following:

a. Agency Governance Roles and Bodies

Consistent with agency policies, the Federal workforce is encouraged to embrace AI adoption at all levels of the Federal Government and to use AI for innovation and increased efficiency. To support this adoption and use, senior agency leaders must effectively distribute responsibilities and accountability, collaborating with agency officials in AI and AI-enabling roles. In support of these objectives and consistent with Executive Order 13960 and Executive Order 14179, agency heads are responsible for establishing the following:

i. Chief AI Officers. Within 60 days of the issuance of this memorandum, the head of each agency must retain or designate a Chief AI Officer (CAIO). CAIOs will promote AI innovation, adoption, and governance, in coordination with appropriate agency officials. Agency heads may choose to designate an existing official, such as a Chief Information Officer, Chief Data Officer, Chief Technology Officer, or similar official with relevant or complementary authorities and responsibilities, provided that individual has significant expertise in AI.

For CFO Act agencies, the CAIO must hold a position at the Senior Executive Service, Scientific and Professional, or Senior Leader level, or equivalent. For other agencies, the CAIO must be at or above Grade 14 of the General Schedule (GS), or the equivalent for agencies that do not use the GS classification system. CAIOs must have the necessary authority to perform the responsibilities in this section and must be positioned highly enough to engage regularly with other agency leadership, to include the Deputy Secretary or equivalent. Agencies must notify OMB within 30 days when the designated CAIO changes or the position is vacant. CAIOs, in coordination with appropriate agency officials, must:

A. promote agency-wide responsible AI innovation and adoption in accordance with this memorandum through a governance and oversight process;
B. coordinate with other responsible agency officials to ensure that the agency's use of AI complies with applicable law and governmentwide guidance;
C. serve as the senior advisor on AI to the head of the agency and within their agency's executive decision-making forums;
D. represent their agency in and collaborate with coordination bodies related to their agency's AI activities, including external forums such as AI-related councils, standard-setting bodies, relevant governance boards, or international bodies;

Marvell Semiconductor, Inc. - Ex. 1046, Page 000010

E. maintain the agency's AI Use Case Inventory;[20]
F. ensure processes are in place for the agency's high-impact AI use, consistent with Section 4 of this memorandum, by:
    1. establishing a process for determining and documenting AI use cases as high-impact;
    2. establishing processes to measure, monitor, and evaluate the ongoing performance and effectiveness of the agency's high-impact AI applications;
    3. overseeing agency compliance with requirements to manage risks from the use of AI, including those established in this memorandum and in relevant law and policy;
    4. establishing a process for an independent review of high-impact use cases before risk acceptance, consistent with Section 4;
    5. centrally tracking high-impact use cases and use case determinations;
G. advise on the transformation of the agency's workforce into an AI-ready workforce;
H. ensure that custom-developed AI code and the data used to develop and test AI are appropriately inventoried, shared, and released in agency code and data repositories, in coordination with their agency's relevant officials;
I. provide guidance on AI investments to the agency head and agency CFO related to resourcing requirements necessary to implement this memorandum; and
J. support agency efforts to track AI spending.

ii. Agency AI Governance Board. Within 90 days of the issuance of this memorandum, each CFO Act agency must convene its relevant agency officials to coordinate and govern issues related to the use of AI within the Executive Branch. Agencies are permitted to rely on existing governance bodies to fulfill this requirement. Agencies are responsible for ensuring that agency AI governance boards:

A. include a chair, at the Deputy Secretary level or equivalent, and a vice-chair who is the agency CAIO. Working through this Board, CAIOs will support their respective Deputy Secretaries in coordinating agency AI activities;
B. include appropriate representation from key stakeholder offices or components, including those responsible for addressing IT, cybersecurity, data, budget, statistics, legal counsel, privacy, civil rights, and civil liberties. When relevant, AI governance boards must include representatives from the following disciplines: agency management, human capital, procurement, customer experience, program evaluation, and officials responsible for implementing AI within an agency's program office(s); and
C. consult external experts, as needed and appropriate, to broaden the perspective of the designated governance board and to integrate sector-specific expertise, including recommendations on innovative agency AI use cases.

[20] As required by Pub. L. No. 117-263, div. G, title LXXII, subtitle B, § 7225 (codified at 40 U.S.C. 11301 note), https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000011

b. Agency Governance Responsibilities

Agencies must enable responsible AI governance and ensure innovative and appropriate use of AI agency-wide. Agency heads must:

i. Empower Agency AI Leaders. Agencies must enable trained and accountable agency officials at the lowest appropriate level[21] to identify, assess, mitigate, and accept risk for AI use cases.[22]

ii. Develop Compliance Plans. Consistent with Section 104(c) and (d) of the AI in Government Act of 2020, within 180 days of the issuance of this memorandum or any update to this memorandum, and every two years thereafter until 2036, each agency must submit to OMB and post publicly on the agency's website either a plan to achieve consistency with this memorandum, or a written determination that the agency does not use and does not anticipate using covered AI. Agencies must also include plans to update any existing internal AI principles and guidelines to ensure consistency with this memorandum.[23] OMB will provide templates for these compliance plans.

iii. Update Agency Policies. Within 270 days of the issuance of this memorandum, agencies must revisit and update where necessary their internal policies on IT infrastructure (e.g., software tools, use of open source software, libraries, and code for AI development, software deployment and platform modernization), data (e.g., data inventory; making quality data available for use by AI; lawful access to agency data, third-party data, and publicly available data, where appropriate; representativeness), cybersecurity (e.g., information system authorizations, continuous monitoring, continuous authorizations for AI), and privacy to align with this memorandum, Executive Order 14179, Executive Order 13960, and with applicable law. Agency policies should aim to advance using models that are built with less data, require less compute, and are inherently more explainable, where possible.

iv. Develop Generative AI Policy. Within 270 days of the issuance of this memorandum, agencies should develop a policy that sets the terms for acceptable use of generative AI for their missions and establishes adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk.

v. Update AI Use Case Inventories. Each agency (except for the Department of Defense and the Intelligence Community) must inventory its AI use cases at least annually, submit the inventory to OMB, and post a public version on the agency's website. Agencies are encouraged to update the public versions of their inventories on an ongoing basis to reflect

[21] Agencies are encouraged to assign these responsibilities to agency officials who are accountable for the mission outcome of the AI use case.

[22] The process for reviewing and accepting risk for AI use cases is separate from, and does not supersede, the authorization process for information systems, consistent with OMB Circular No. A-130, Managing Information as a Strategic Resource, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

[23] Given the importance of context-specific guidance on AI, agencies are encouraged to continue implementing their agency's AI principles and guidelines, so long as they do not conflict with this memorandum.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000012

their current use of AI. OMB will issue detailed instructions to agencies regarding the inventory and its scope.

c. Federal Governance Roles and Bodies

Breaking barriers to AI adoption and ensuring the government is maximizing efficiency requires coordination. The primary interagency body to lead this coordination will be the Chief AI Officer Council.

i. Chief AI Officer Council. Within 90 days of the issuance of this memorandum, the Director of OMB, or designated senior official within OMB, shall convene and chair an interagency council to coordinate the development and use of AI in agencies' programs and operations, other than the use of AI in national security systems, and to advance the implementation of the AI Principles established by Section 6 of Executive Order 13960. The Chief AI Officer Council shall:

A. include as members the Chief AI Officers of CFO Act agencies, as well as representatives of the White House Office of Science and Technology Policy, the Office of the Director of National Intelligence, and other agencies as identified by the Chair;
B. coordinate the development and use of AI across agencies' programs and operations, including enabling compliance with implementation of this memorandum and all other applicable authorities;
C. develop and promote shared templates, formats, technical resources, and exemplary uses of agency AI adoption and implementation; and
D. sunset five years after the issuance of this memorandum, unless otherwise authorized by the OMB Director.

4. FOSTERING PUBLIC TRUST IN FEDERAL USE OF AI

Agencies must continue to develop AI that serves the public by, for example, increasing the accessibility of government services, increasing government efficiency, enhancing national security, and growing American economic competitiveness in a way that benefits people across the United States. Agencies must ensure their AI use is trustworthy, secure, and accountable, in accordance with Executive Order 13960. In the pursuit of agency-wide AI adoption and use, the Federal workforce at varying levels will participate in AI or AI-enabling roles, with accountable officials assuming risk.[24] As part of this effort, AI risk management policies must be written to both ensure the minimum number of requirements necessary to enable the trustworthy and responsible use of AI and also ensure those requirements are understandable and implementable.

Agencies are required to implement minimum risk management practices, detailed in Section 4(b) of this memorandum, to manage risks from high-impact AI use cases. However, Sections 4(a) through (b) of this memorandum do not apply to elements of the Intelligence

[24] Agencies are encouraged to assign these responsibilities to agency officials who are accountable for the mission outcome of the AI use case.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000013

Community.[25] Consistent with these goals, agencies must undertake the following, in addition to following OMB standards and requirements governing information dissemination, where applicable.[26]

a. Determining High-Impact AI

This section introduces requirements that are *only* applicable to "high-impact" agency uses of AI. As further defined in Section 5 of this memorandum, 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. As part of conducting internal reviews of high-impact use, agencies should evaluate the AI's specific output and its potential risks when assessing the applicability of the high-impact definition.[27] A high-impact determination is possible whether there is or is not human oversight for the decision or action.[28]

Section 6 provides agencies with categories of AI use cases that are automatically presumed to be high-impact. For AI use cases in these categories, an appropriate agency official must submit written documentation to notify the CAIO when making a determination that a particular AI use case does not actually meet the definition of high-impact. CAIOs are responsible for providing such determinations to OMB upon request. Agencies are also encouraged to identify additional context-specific risks that are associated with their use of such AI and address them as appropriate. CAIOs may revisit any determinations made within their agency to conclude that an AI use case is considered "high-impact" and must be subject to the minimum risk management practices at any time.

The practices in this section represent an initial baseline for managing risk from the implementation of high-impact AI use cases.[29] Agencies are also encouraged to continue developing their own agency-specific practices, as appropriate and consistent with this memorandum and the principles in Executive Orders 13960 and 14179. Where possible, agencies should streamline approvals for intended use cases that are closely related in their deployment context and have substantially similar risk profiles. In implementing AI risk management for high-impact AI use cases, agencies and their CAIOs are responsible for the following:

i. Implementing Risk Management Practices and Termination of Non-Compliant AI. Within 365 days of the issuance of this memorandum, agencies must document implementation of the minimum practices in Section 4(b) of this memorandum for high-impact uses of AI and be prepared to report them to OMB, as part of periodic accountability reviews, the annual AI use case inventory, or upon request as determined

[25] Although elements of the Intelligence Community are not required to implement these practices, they are encouraged to do so.

[26] See OMB Memorandum M-19-15, *Improving Implementation of the Information Quality Act,* https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/04/M-19-15.pdf.

[27] AI may be integrated in decision or activity pipelines in high-impact categories without meeting the definition of high-impact because the AI's output does not actually "serve as a principal basis for" the relevant type of agency action or decision, as described in this memorandum's definition of "high-impact AI." *See* Section 5.

[28] Additional details are provided in Section 6 to assist with risk determinations for high-impact AI.

[29] For AI systems, agencies must continue to follow applicable authorization to operate requirements from OMB Circular No. A-130, *Managing Information as a Strategic Resource.*

Marvell Semiconductor, Inc. - Ex. 1046, Page 000014

by OMB. If a particular high-impact use case is not compliant with the minimum practices then the agency must safely discontinue use of the AI functionality.

Pilot programs for a proposed AI use case are exempt from the minimum risk management practices, provided that:

A. the program is of limited scale and duration;
B. the agency CAIO has certified that the pilot may go forward, and that certification is tracked centrally;
C. when possible, individuals who may interact with the AI have the ability to opt into and out of participating in the pilot, with sufficient notice to make an informed decision; and
D. minimum risk management practices are applied where practicable.

ii. Authorizing Waivers from Minimum Practices for High-Impact AI. In coordination with other relevant officials, an agency CAIO may waive one or more of the requirements in this section for a specific covered AI application or component after making a written determination, based upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. An agency CAIO, in coordination with other relevant officials, must certify the ongoing validity of each waiver on an annual basis, and may also revoke a previously issued waiver at any time. The CAIO's responsibility under this paragraph shall not be delegated down to other officials.

iii. Tracking Waivers from Minimum Practices for High-Impact AI. In addition to the certification and publication requirements in Section 4(a)(ii) and Section 4(a)(iv) of this memorandum, CAIOs must centrally track waivers, reassess them if there are significant changes to the conditions or context in which the AI is used, and within 30 days of granting or revoking any waiver, report to OMB on the scope, justification, and evidence supporting that action.

iv. Publicly Reporting Determinations and Waivers. To the extent consistent with law and governmentwide policy, each agency must publicly release a summary describing each individual determination and waiver, as well its justification. OMB will issue detailed instructions for these summaries. Alternatively, agencies must publicly indicate, if the agency has no active determinations or waivers.

b. Implementing Minimum Risk Management Practices for High-Impact AI

Agencies must implement the following minimum risk management practices for high-impact AI use cases:

i. Conduct Pre-Deployment Testing. Agencies must develop pre-deployment testing and prepare risk mitigation plans that reflect expected real-world outcomes and identify expected benefits to the AI use. In conducting pre-deployment testing, if an agency does not have access to the underlying AI source code, models, or data, the agency must use

Marvell Semiconductor, Inc. - Ex. 1046, Page 000015

alternative test methodologies, such as querying the AI service and observing the outputs or providing evaluation data to the vendor and obtaining results.

ii. Complete AI Impact Assessment. Agencies must complete an AI impact assessment before deploying any high-impact AI use case. These assessments must be updated periodically and throughout the AI's lifecycle, as appropriate, using target variables that anticipate real-world outcomes. The AI impact assessments must be documented and address or include, at a minimum:

A. *the intended purpose for the AI and its expected benefit,* supported by specific metrics or qualitative analysis, assessing impact inclusive of but not limited to costs, customer experience, or expected positive outcomes of AI use, as compared to existing agency processes;

B. *the quality and appropriateness of the relevant data and model capability,* supported by a summary of the data used in the AI's design, development, training, testing, and operation and its fitness for the AI's intended purpose; describe the data collection, and preparation process; and indicate whether the data is to be publicly disclosed as an open government data asset. When applicable, this summary must describe information included in the data about classes protected by Federal nondiscrimination laws;

C. *the potential impacts of using AI*, supported by documentation on potential impacts on the privacy, civil rights, and civil liberties of the public, and of using or not using AI. The assessment should reference privacy impact assessments, CAIO-approved minimum risk management practice waivers or other materials, if relevant, and also describe any planned mitigation measures for anticipated negative impacts, such as unlawful discrimination;[30]

D. *reassessment scheduling and procedures*, supported by schedules for periodic reassessments as well as reassessment requirements following significant modifications to an underlying AI system, in addition to the specific requirements and processes for such testing;

E. *related costs analysis*, supported by a summary of direct costs associated and expected savings, if any;

F. *results of independent review,* supported by an independent reviewer within the agency who has not been involved in the development. The independent reviewer of the impact assessment shall identify any potential concerns or gaps. Any comments provided by the independent reviewer must be included in the impact assessment documentation and shared with the individual accepting the risk for the AI use case when that determination is made; and

[30] Pub. L. No. 107-347, § 208 and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000016

G. *risk acceptance,* supported by a signature from the individual accepting the risk.

iii. Conduct Ongoing Monitoring for Performance and Potential Adverse Impacts. Agencies must conduct testing and periodic human review of AI use cases, where feasible, to identify any adverse impacts to the performance and security of AI functionality, including those that may violate laws governing privacy, civil rights, or civil liberties. Ongoing monitoring must be designed to detect unforeseen circumstances, changes to an AI system after deployment, or changes to the context of use or associated data. Agencies must implement appropriate mitigations and ensure proper system and use documentation; and where possible, develop processes enabling traceability and transparency in this evaluation.

iv. Ensure Adequate Human Training and Assessment. Agencies must ensure there is sufficient and periodic training, assessment, and oversight for operators of AI to interpret and act on the AI's output and manage associated risks. Training should be conducted on a periodic basis, as determined by the agency, and should be specific to the AI system or service being operated and how it is being used.

v. Provide Additional Human Oversight, Intervention, and Accountability. Agencies must ensure human oversight, intervention, and accountability suitable for high-impact use cases. When practicable and consistent with existing agency practices, agencies must ensure that the AI functionality has an appropriate fail-safe that minimizes the risk of significant harm.[31]

vi. Offer Consistent Remedies or Appeals. Agencies must ensure that individuals affected by AI-enabled decisions have access to a timely human review and a chance to appeal any negative impacts, when appropriate. If an agency already has an appeals or human review process in place, such as appeals of adverse actions, it may extend or adapt that process to cover decisions made with AI, consistent with applicable law. Any remedy process should be designed to avoid placing unnecessary burdens on the individual and should follow established guidance for minimizing administrative burdens.

vii. Consult and Incorporate Feedback from End Users and the Public. Agencies must provide an option for end users and the public to submit feedback on the use case, where appropriate, in the design, development, and use of the AI and use such feedback to inform agency decision-making regarding the AI (refer to Section 8 of this memorandum).

[31] For example, an AI-enabled safety mechanism may require an immediate and automated action to prevent a harm from occurring. It would not be practicable in this case to require human intervention to approve the activation of the safety mechanism. However, agencies must still determine the appropriate oversight and accountability processes for such a use of AI.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000017

5. DEFINITIONS

The below definitions apply for the purposes of this memorandum.

Agency: The term "agency" has the meaning provided in 44 U.S.C. § 3502(1).

Artificial Intelligence (AI): The term "artificial intelligence" has the meaning provided in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[32]

For the purposes of this memorandum, the following technical context should guide interpretation of the definition above:

1. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
2. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.
3. For this definition, no system should be considered too simple to qualify as covered AI due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).
4. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

AI and AI-Enabling Roles: The term "AI and AI-enabling roles" refers to positions whose major duties include contributions that are important for successful and responsible AI outcomes. AI and AI-Enabling Roles include both technical and non-technical roles, such as data scientists, software engineers, data engineers, data governance specialists, privacy officials, statisticians, machine learning engineers, applied scientists, designers, economists, operations researchers, product managers, policy analysts, program managers, behavioral and social scientists, customer experience strategists, human resource specialists, contracting officials, managers, and attorneys.

AI Maturity: The term "AI maturity" refers to a Federal Government organization's capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with relevant Federal law, regulation, and policy on AI.

AI Model: The term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

AI System: The term "AI system" has the definition provided in Section 7223 of the Advancing American AI Act, which states that "[t]he term 'artificial intelligence system'— (A) means any

[32] Pub. L. No. 115-232, § 238(g), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000018

data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, whether— (i) the data system, software, application, tool, or utility is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; or (ii) artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and (B) does not include any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system."

Applied Research: The term "applied research" refers to original investigation undertaken in order to acquire new knowledge to determine the means by which a specific practical aim or objective may be met.

Basic Research: The term "basic research" refers to experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts without a specific application towards processes or products in mind.

Custom-Developed Code: The term "custom-developed code" has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Customer Experience: The term "customer experience" means the public's perceptions of, and overall satisfaction with, the interactions with an agency, product, or service.

Data Asset: The term "data asset" has the meaning provided in 44 U.S.C § 3502.

Federal Information: The term "Federal information" has the meaning provided in OMB Circular A-130.

High-Impact AI: AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on:

1. an individual or entity's civil rights, civil liberties, or privacy; or
2. an individual or entity's access to education, housing, insurance, credit, employment, and other programs;
3. an individual or entity's access to critical government resources or services;
4. human health and safety;
5. critical infrastructure or public safety; or
6. strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

Information Technology: The term "information technology" has the definition given in 40 U.S.C. § 11101(6).

Model Weight: The term "model weight" means a numerical parameter within an AI model that helps determine the model's outputs in response to inputs.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000019

National Security System: The term "National Security System" has the meaning provided in 44 U.S.C. § 3552(b)(6).

Open Government Data Asset: The term "open government data asset" has the meaning provided in 44 U.S.C § 3502.

Open Source Software: The term "open source software" has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Significant Modification: The term "significant modification" refers to an update to an AI application or to the conditions or context in which it is used, such as through changing its functionality, underlying structure, or performance, that meaningfully alters the AI's impact, rendering prior evaluations, training, or documentation misleading to users, overseers, or individuals affected by the system. This includes significantly changing the context, scope, or intended purpose in which the AI is used.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000020

6. PURPOSES FOR WHICH AI IS PRESUMED TO BE HIGH-IMPACT

The following is a list of categories for which the use or expected use of AI that serves as a principal basis for an agency decision or action is presumed to be high-impact. However, the following is not an exhaustive list of potentially high-impact AI use cases and agencies should base any final decisions for whether an AI use case is high-impact on the definition provided in Section 6.

a. Safety-critical functions of critical infrastructure or government facilities, emergency services, fire and life safety systems within structures, food safety mechanisms, or traffic control systems and other systems controlling physical transit;
b. Physical movements of robots, robotic appendages, vehicles or craft (whether land, sea, air, or underground), or industrial equipment that have the potential to cause significant injury to humans;
c. Use of kinetic or non-kinetic measures for attack or active defense in real world circumstances that could cause significant injury to humans;
d. Transport, safety, design, development, or use of hazardous chemicals or biological agents;
e. Design, construction, or testing of equipment, systems, or public infrastructure that would pose a significant risk to safety if they failed;
f. In healthcare contexts, the medically relevant functions of medical devices; patient diagnosis, risk assessment, or treatment; the allocation of care in the context of public insurance; or the control of health-insurance costs and underwriting;
g. Control of access to, or the security of, government facilities;
h. Adjudication or enforcement of sanctions, trade restrictions, or other controls on exports, investments, or shipping;
i. The blocking, removal, hiding, or limitation of the reach of protected speech;
j. In law enforcement contexts, production of risk assessments about individuals; identification of criminal suspects; forecast of crime; tracking of non-governmental vehicles over time in public spaces; application of biometric identification (e.g., iris, facial, fingerprint, or gait matching); facial reconstruction based on genetic information; social media monitoring; application of digital forensic techniques; use of cyber intrusions; physical location-monitoring or tracking of individuals; detection of weapons or violent activity; or determinations related to recidivism, sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention;
k. Preparation or adjudication of risk assessments related to foreign nationals seeking temporary or permanent access to the U.S. or its territories including related to immigration, asylum, detention, or travel approval status;
l. Use of biometric identification for one-to-many identification in publicly accessible spaces;
m. Ability to apply for, or adjudication of, requests for critical federal services, processes, and benefits to include loans and access to public housing; determination of continued eligibility for ongoing benefits; the control of access—through biometrics or other means (e.g., signature matching)—to IT systems for accessing services for benefits; detection of fraudulent use or attempted use of government services; adjudication of penalties in the context of government benefits;

Marvell Semiconductor, Inc. - Ex. 1046, Page 000021

n. Determination of the terms or conditions of Federal employment, including pre-employment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; reassignment of workers to new tasks or teams; or
o. Provision of language translation (e.g., foreign translation and audiovisual translation) when responses are legally binding or for an interaction that directly informs an agency decision or action.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000022

7. METHODS OF UNDERSTANDING AI RISK MANAGEMENT

Below are ways in which risks may arise from the use of AI. The term "risks from the use of AI" refers to risks related to efficacy, safety, fairness, transparency, accountability, appropriateness, or lawfulness of a decision or action resulting from the use of AI to inform, influence, decide, or execute that decision or action.

This includes such risks regardless of whether:

1. the AI merely informs the decision or action, partially automates it, or fully automates it;
2. there is or is not human oversight for the decision or action;
3. it is or is not readily apparent that a decision or action took place, such as when an AI application performs a background task or silently declines to take an action; or
4. the humans involved in making the decision or action or that are affected by it are or are not aware of how or to what extent the AI influenced or automated the decision or action.

The following factors can create, contribute to, or exacerbate risks from the use of AI:

1. AI outputs that are inaccurate or misleading;
2. AI outputs that are unreliable, ineffective, or not robust;
3. AI outputs that discriminate on the basis of a protected characteristic;
4. AI outputs that contribute to actions or decisions resulting in harmful or unsafe outcomes, including AI outputs that lower the barrier for people to take intentional and harmful actions;
5. AI being used for tasks to which it is poorly suited or being inappropriately repurposed in a context for which it was not intended;
6. AI being used in a context in which affected people have a reasonable expectation that a human is or should be primarily responsible for a decision or action; and
7. the adversarial evasion or manipulation of AI, as in the case of an entity purposefully inducing AI to misclassify an input.

This definition applies to risks specifically arising from using AI and that affect the outcomes of decisions or actions. It does not include all risks associated with AI, such as risks related to the privacy, security, and confidentiality of the data used to train AI or used as inputs to AI models.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000023

8. Public Consultation and Feedback

To carry out public consultations and feedback processes, agencies are recommended to take appropriate steps to solicit public input, which could include:[33]

1. direct usability testing, such as observing users interacting with the system;
2. general solicitations of comments from the public, such as a request for information in the *Federal Register* or a "Tell Us About Your Experience" sheet with an open-ended space for responses;
3. post-transaction customer feedback collections;[34]
4. public hearings or meetings; and
5. any other transparent process that seeks public input, comments, or feedback from the affected groups in a meaningful, accessible, and effective manner.

[33] Agencies are encouraged to engage with OMB on whether they are required to submit information collection requests for OMB clearance under the Paperwork Reduction Act (44 U.S.C. § 3507), https://uscode.house.gov/view.xhtml?req=44+U.S.C.+%EF%BF%BD+3507&f=treesort&fq=true&num=20&hl=true&edition=prelim&granuleId=USC-prelim-title44-section3507, for the purposes of these consultations and feedback processes.

[34] Information on post-transaction customer feedback surveys can be found in OMB Circular A-11, Section 280 – Managing Customer Experience and Improving Service Delivery, https://www.performance.gov/cx/assets/files/2019_a11%20280.pdf.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000024

Consolidated Table of Actions

Responsible Entity	*Action*	*Section*	*Deadline*
Each Agency	Retain or designate a Chief AI Officer.	3(a)(i)	60 days
Each CFO Act Agency	Convene relevant agency officials to coordinate and govern issues tied to the use of AI within the Federal Government through an agency AI Governance Board.	3(a)(ii)	90 days
OMB	Convene a Chief AI Officer Council, led by the Director of OMB, or designated senior official.	3(c)(i)	90 days
Each CFO Act Agency	Develop and release publicly an agency strategy for removing barriers to the use of AI and advancing agency AI maturity.	2(a)	180 days
Each Agency	Submit to OMB and release publicly an agency compliance plan to achieve consistency with this memorandum, or a written determination that the agency does not use and does not anticipate using covered AI.	3(b)(ii)	180 days, and every two years until 2036
Each Agency	Update internal policies on IT infrastructure, data, cybersecurity, and privacy.	3(b)(iii)	270 days
Each Agency	Develop a Generative AI policy.	3(b)(iv)	270 days
Each Agency*	Implement the minimum risk management practices for high-impact uses of AI.	4(a)(i)	365 days
Each Agency*	Report directly to OMB any determinations and waivers that are granted or revoked.	4(a)(iii)	Annually and 30-days after significant modifications
Each Agency*	Publicly report determinations and waivers for AI use cases.	4(a)(iv)	365 days
Each Agency**	Publicly release an AI use case inventory consistent with OMB instructions.	3(b)(v)	Annually

* Excluding elements of the Intelligence Community.
** Excluding elements of the Intelligence Community. The Department of Defense is exempt from the requirement to inventory individual use cases.

Marvell Semiconductor, Inc. - Ex. 1046, Page 000025