

Administration of Joseph R. Biden, Jr., 2024

National Security Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence To Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence

October 24, 2024

National Security Memorandum/NSM-25

Memorandum for the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Energy, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Director of National Intelligence, the Representative of the United States of America to the United Nations, the Director of the Central Intelligence Agency, the Assistant to the President and Chief of Staff, the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy and Director of the National Economic Council, the Chair of the Council of Economic Advisers, the Director of the Office of Science and Technology Policy, the Administrator of the United States Agency for International Development, the Director of the National Science Foundation, the Director of the Federal Bureau of Investigation, the National Cyber Director, the Director of the Office of Pandemic Preparedness and Response Policy, the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, and the Director of the Defense Intelligence Agency

Subject: Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence

Section 1. Policy. (a) This memorandum fulfills the directive set forth in subsection 4.8 of Executive Order 14110 of October 30, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). This memorandum provides further direction on appropriately harnessing artificial intelligence (AI) models and AI-enabled technologies in the United States Government, especially in the context of national security systems (NSS), while protecting human rights, civil rights, civil liberties, privacy, and safety in AI-enabled national security activities. A classified annex to this memorandum addresses additional sensitive national security issues, including countering adversary use of AI that poses risks to United States national security.

(b) United States national security institutions have historically triumphed during eras of technological transition. To meet changing times, they developed new capabilities, from submarines and aircraft to space systems and cyber tools. To gain a decisive edge and protect national security, they pioneered technologies such as radar, the Global Positioning System, and nuclear propulsion, and unleashed these hard-won breakthroughs on the battlefield. With each paradigm shift, they also developed new systems for tracking and countering adversaries' attempts to wield cutting-edge technology for their own advantage.

(c) AI has emerged as an era-defining technology and has demonstrated significant and growing relevance to national security. The United States must lead the world in the responsible application of AI to appropriate national security functions. AI, if used appropriately and for its intended purpose, can offer great benefits. If misused, AI could threaten United States national security, bolster authoritarianism worldwide, undermine democratic institutions and processes,

facilitate human rights abuses, and weaken the rules-based international order. Harmful outcomes could occur even without malicious intent if AI systems and processes lack sufficient protections.

(d) Recent innovations have spurred not only an increase in AI use throughout society, but also a paradigm shift within the AI field—one that has occurred mostly outside of Government. This era of AI development and deployment rests atop unprecedented aggregations of specialized computational power, as well as deep scientific and engineering expertise, much of which is concentrated in the private sector. This trend is most evident with the rise of large language models, but it extends to a broader class of increasingly general-purpose and computationally intensive systems. The United States Government must urgently consider how this current AI paradigm specifically could transform the national security mission.

(e) Predicting technological change with certainty is impossible, but the foundational drivers that have underpinned recent AI progress show little sign of abating. These factors include compounding algorithmic improvements, increasingly efficient computational hardware, a growing willingness in industry to invest substantially in research and development, and the expansion of training data sets. AI under the current paradigm may continue to become more powerful and general-purpose. Developing and effectively using these systems requires an evolving array of resources, infrastructure, competencies, and workflows that in many cases differ from what was required to harness prior technologies, including previous paradigms of AI.

(f) If the United States Government does not act with responsible speed and in partnership with industry, civil society, and academia to make use of AI capabilities in service of the national security mission—and to ensure the safety, security, and trustworthiness of American AI innovation writ large—it risks losing ground to strategic competitors. Ceding the United States' technological edge would not only greatly harm American national security, but it would also undermine United States foreign policy objectives and erode safety, human rights, and democratic norms worldwide.

(g) Establishing national security leadership in AI will require making deliberate and meaningful changes to aspects of the United States Government's strategies, capabilities, infrastructure, governance, and organization. AI is likely to affect almost all domains with national security significance, and its use cannot be relegated to a single institutional silo. The increasing generality of AI means that many functions that to date have been served by individual bespoke tools may, going forward, be better fulfilled by systems that, at least in part, rely on a shared, multi-purpose AI capability. Such integration will only succeed if paired with appropriately redesigned United States Government organizational and informational infrastructure.

(h) In this effort, the United States Government must also protect human rights, civil rights, civil liberties, privacy, and safety, and lay the groundwork for a stable and responsible international AI governance landscape. Throughout its history, the United States has been a global leader in shaping the design, development, and use of new technologies not only to advance national security, but also to protect and promote democratic values. The United States Government must develop safeguards for its use of AI tools, and take an active role in steering global AI norms and institutions. The AI frontier is moving quickly, and the United States Government must stay attuned to ongoing technical developments without losing focus on its guiding principles.

(i) This memorandum aims to catalyze needed change in how the United States Government approaches AI national security policy. In line with Executive Order 14110, it directs actions to strengthen and protect the United States AI ecosystem; improve the safety, security, and trustworthiness of AI systems developed and used in the United States; enhance the United States

Government's appropriate, responsible, and effective adoption of AI in service of the national security mission; and minimize the misuse of AI worldwide.

Sec. 2. Objectives. It is the policy of the United States Government that the following three objectives will guide its activities with respect to AI and national security.

(a) First, the United States must lead the world's development of safe, secure, and trustworthy AI. To that end, the United States Government must—in partnership with industry, civil society, and academia—promote and secure the foundational capabilities across the United States that power AI development. The United States Government cannot take the unmatched vibrancy and innovativeness of the United States AI ecosystem for granted; it must proactively strengthen it, ensuring that the United States remains the most attractive destination for global talent and home to the world's most sophisticated computational facilities. The United States Government must also provide appropriate safety and security guidance to AI developers and users, and rigorously assess and help mitigate the risks that AI systems could pose.

(b) Second, the United States Government must harness powerful AI, with appropriate safeguards, to achieve national security objectives. Emerging AI capabilities, including increasingly general-purpose models, offer profound opportunities for enhancing national security, but employing these systems effectively will require significant technical, organizational, and policy changes. The United States must understand AI's limitations as it harnesses the technology's benefits, and any use of AI must respect democratic values with regard to transparency, human rights, civil rights, civil liberties, privacy, and safety.

(c) Third, the United States Government must continue cultivating a stable and responsible framework to advance international AI governance that fosters safe, secure, and trustworthy AI development and use; manages AI risks; realizes democratic values; respects human rights, civil rights, civil liberties, and privacy; and promotes worldwide benefits from AI. It must do so in collaboration with a wide range of allies and partners. Success for the United States in the age of AI will be measured not only by the preeminence of United States technology and innovation, but also by the United States' leadership in developing effective global norms and engaging in institutions rooted in international law, human rights, civil rights, and democratic values.

Sec. 3. Promoting and Securing the United States' Foundational AI Capabilities. (a) To preserve and expand United States advantages in AI, it is the policy of the United States Government to promote progress, innovation, and competition in domestic AI development; protect the United States AI ecosystem against foreign intelligence threats; and manage risks to AI safety, security, and trustworthiness. Leadership in responsible AI development benefits United States national security by enabling applications directly relevant to the national security mission, unlocking economic growth, and avoiding strategic surprise. United States technological leadership also confers global benefits by enabling like-minded entities to collectively mitigate the risks of AI misuse and accidents, prevent the unchecked spread of digital authoritarianism, and prioritize vital research.

3.1. Promoting Progress, Innovation, and Competition in United States AI Development. (a) The United States' competitive edge in AI development will be at risk absent concerted United States Government efforts to promote and secure domestic AI progress, innovation, and competition. Although the United States has benefited from a head start in AI, competitors are working hard to catch up, have identified AI as a top strategic priority, and may soon devote resources to research and development that United States AI developers cannot match without appropriately supportive Government policies and action. It is therefore the policy of the United States Government to enhance innovation and competition by bolstering key drivers of AI progress, such as technical talent and computational power.

(b) It is the policy of the United States Government that advancing the lawful ability of noncitizens highly skilled in AI and related fields to enter and work in the United States constitutes a national security priority. Today, the unparalleled United States AI industry rests in substantial part on the insights of brilliant scientists, engineers, and entrepreneurs who moved to the United States in pursuit of academic, social, and economic opportunity. Preserving and expanding United States talent advantages requires developing talent at home and continuing to attract and retain top international minds.

(c) Consistent with these goals:

(i) On an ongoing basis, the Department of State, the Department of Defense (DOD), and the Department of Homeland Security (DHS) shall each use all available legal authorities to assist in attracting and rapidly bringing to the United States individuals with relevant technical expertise who would improve United States competitiveness in AI and related fields, such as semiconductor design and production. These activities shall include all appropriate vetting of these individuals and shall be consistent with all appropriate risk mitigation measures. This tasking is consistent with and additive to the taskings on attracting AI talent in section 5 of Executive Order 14110.

(ii) Within 180 days of the date of this memorandum, the Chair of the Council of Economic Advisers shall prepare an analysis of the AI talent market in the United States and overseas, to the extent that reliable data is available.

(iii) Within 180 days of the date of this memorandum, the Assistant to the President for Economic Policy and Director of the National Economic Council shall coordinate an economic assessment of the relative competitive advantage of the United States private sector AI ecosystem, the key sources of the United States private sector's competitive advantage, and possible risks to that position, and shall recommend policies to mitigate them. The assessment could include areas including (1) the design, manufacture, and packaging of chips critical in AI-related activities; (2) the availability of capital; (3) the availability of workers highly skilled in AI-related fields; (4) computational resources and the associated electricity requirements; and (5) technological platforms or institutions with the requisite scale of capital and data resources for frontier AI model development, as well as possible other factors.

(iv) Within 90 days of the date of this memorandum, the Assistant to the President for National Security Affairs (APNSA) shall convene appropriate executive departments and agencies (agencies) to explore actions for prioritizing and streamlining administrative processing operations for all visa applicants working with sensitive technologies. Doing so shall assist with streamlined processing of highly skilled applicants in AI and other critical and emerging technologies. This effort shall explore options for ensuring the adequate resourcing of such operations and narrowing the criteria that trigger secure advisory opinion requests for such applicants, as consistent with national security objectives.

(d) The current paradigm of AI development depends heavily on computational resources. To retain its lead in AI, the United States must continue developing the world's most sophisticated AI semiconductors and constructing its most advanced AI-dedicated computational infrastructure.

(e) Consistent with these goals:

(i) DOD, the Department of Energy (DOE) (including national laboratories), and the Intelligence Community (IC) shall, when planning for and constructing or renovating computational facilities, consider the applicability of large-scale AI to their mission.

Where appropriate, agencies shall design and build facilities capable of harnessing frontier AI for relevant scientific research domains and intelligence analysis. Those investments shall be consistent with the Federal Mission Resilience Strategy adopted in Executive Order 13961 of December 7, 2020 (Governance and Integration of Federal Mission Resilience).

(ii) On an ongoing basis, the National Science Foundation (NSF) shall, consistent with its authorities, use the National AI Research Resource (NAIRR) pilot project and any future NAIRR efforts to distribute computational resources, data, and other critical assets for AI development to a diverse array of actors that otherwise would lack access to such capabilities—such as universities, nonprofits, and independent researchers (including trusted international collaborators)—to ensure that AI research in the United States remains competitive and innovative. This tasking is consistent with the NAIRR pilot assigned in section 5 of Executive Order 14110.

(iii) Within 180 days of the date of this memorandum, DOE shall launch a pilot project to evaluate the performance and efficiency of federated AI and data sources for frontier AI-scale training, fine-tuning, and inference.

(iv) The Office of the White House Chief of Staff, in coordination with DOE and other relevant agencies, shall coordinate efforts to streamline permitting, approvals, and incentives for the construction of AI-enabling infrastructure, as well as surrounding assets supporting the resilient operation of this infrastructure, such as clean energy generation, power transmission lines, and high-capacity fiber data links. These efforts shall include coordination, collaboration, consultation, and partnership with State, local, Tribal, and territorial governments, as appropriate, and shall be consistent with the United States' goals for managing climate risks.

(v) The Department of State, DOD, DOE, the IC, and the Department of Commerce (Commerce) shall, as appropriate and consistent with applicable law, use existing authorities to make public investments and encourage private investments in strategic domestic and foreign AI technologies and adjacent fields. These agencies shall assess the need for new authorities for the purposes of facilitating public and private investment in AI and adjacent capabilities.

3.2. Protecting United States AI from Foreign Intelligence Threats. (a) In addition to pursuing industrial strategies that support their respective AI industries, foreign states almost certainly aim to obtain and repurpose the fruits of AI innovation in the United States to serve their national security goals. Historically, such competitors have employed techniques including research collaborations, investment schemes, insider threats, and advanced cyber espionage to collect and exploit United States scientific insights. It is the policy of the United States Government to protect United States industry, civil society, and academic AI intellectual property and related infrastructure from foreign intelligence threats to maintain a lead in foundational capabilities and, as necessary, to provide appropriate Government assistance to relevant non-government entities.

(b) Consistent with these goals:

(i) Within 90 days of the date of this memorandum, the National Security Council (NSC) staff and the Office of the Director of National Intelligence (ODNI) shall review the President's Intelligence Priorities and the National Intelligence Priorities Framework consistent with National Security Memorandum 12 of July 12, 2022 (The President's Intelligence Priorities), and make recommendations to ensure that such priorities improve identification and assessment of foreign intelligence threats to the United

States AI ecosystem and closely related enabling sectors, such as those involved in semiconductor design and production.

(ii) Within 180 days of the date of this memorandum, and on an ongoing basis thereafter, ODNI, in coordination with DOD, the Department of Justice (DOJ), Commerce, DOE, DHS, and other IC elements as appropriate, shall identify critical nodes in the AI supply chain, and develop a list of the most plausible avenues through which these nodes could be disrupted or compromised by foreign actors. On an ongoing basis, these agencies shall take all steps, as appropriate and consistent with applicable law, to reduce such risks.

(c) Foreign actors may also seek to obtain United States intellectual property through gray-zone methods, such as technology transfer and data localization requirements. AI-related intellectual property often includes critical technical artifacts (CTAs) that would substantially lower the costs of recreating, attaining, or using powerful AI capabilities. The United States Government must guard against these risks.

(d) Consistent with these goals:

(i) In furtherance of Executive Order 14083 of September 15, 2022 (Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States), the Committee on Foreign Investment in the United States shall, as appropriate, consider whether a covered transaction involves foreign actor access to proprietary information on AI training techniques, algorithmic improvements, hardware advances, CTAs, or other proprietary insights that shed light on how to create and effectively use powerful AI systems.

3.3. Managing Risks to AI Safety, Security, and Trustworthiness. (a) Current and near-future AI systems could pose significant safety, security, and trustworthiness risks, including those stemming from deliberate misuse and accidents. Across many technological domains, the United States has historically led the world not only in advancing capabilities, but also in developing the tests, standards, and norms that underpin reliable and beneficial global adoption. The United States approach to AI should be no different, and proactively constructing testing infrastructure to assess and mitigate AI risks will be essential to realizing AI's positive potential and to preserving United States AI leadership.

(b) It is the policy of the United States Government to pursue new technical and policy tools that address the potential challenges posed by AI. These tools include processes for reliably testing AI models' applicability to harmful tasks and deeper partnerships with institutions in industry, academia, and civil society capable of advancing research related to AI safety, security, and trustworthiness.

(c) Commerce, acting through the AI Safety Institute (AISI) within the National Institute of Standards and Technology (NIST), shall serve as the primary United States Government point of contact with private sector AI developers to facilitate voluntary pre- and post-public deployment testing for safety, security, and trustworthiness of frontier AI models. In coordination with relevant agencies as appropriate, Commerce shall establish an enduring capability to lead voluntary unclassified pre-deployment safety testing of frontier AI models on behalf of the United States Government, including assessments of risks relating to cybersecurity, biosecurity, chemical weapons, system autonomy, and other risks as appropriate (not including nuclear risk, the assessment of which shall be led by DOE). Voluntary unclassified safety testing shall also, as appropriate, address risks to human rights, civil rights, and civil liberties, such as those related to privacy, discrimination and bias, freedom of expression, and the safety of individuals and groups. Other agencies, as identified in subsection 3.3(f) of this section, shall establish enduring

capabilities to perform complementary voluntary classified testing in appropriate areas of expertise. The directives set forth in this subsection are consistent with broader taskings on AI safety in section 4 of Executive Order 14110, and provide additional clarity on agencies' respective roles and responsibilities.

(d) Nothing in this subsection shall inhibit agencies from performing their own evaluations of AI systems, including tests performed before those systems are released to the public, for the purposes of evaluating suitability for that agency's acquisition and procurement. AISI's responsibilities do not extend to the evaluation of AI systems for the potential use by the United States Government for national security purposes; those responsibilities lie with agencies considering such use, as outlined in subsection 4.2(e) of this memorandum and the associated framework described in that subsection.

(e) Consistent with these goals, Commerce, acting through AISI within NIST, shall take the following actions to aid in the evaluation of current and near-future AI systems:

(i) Within 180 days of the date of this memorandum and subject to private sector cooperation, AISI shall pursue voluntary preliminary testing of at least two frontier AI models prior to their public deployment or release to evaluate capabilities that might pose a threat to national security. This testing shall assess models' capabilities to aid offensive cyber operations, accelerate development of biological and/or chemical weapons, autonomously carry out malicious behavior, automate development and deployment of other models with such capabilities, and give rise to other risks identified by AISI. AISI shall share feedback with the APNSA, interagency counterparts as appropriate, and the respective model developers regarding the results of risks identified during such testing and any appropriate mitigations prior to deployment.

(ii) Within 180 days of the date of this memorandum, AISI shall issue guidance for AI developers on how to test, evaluate, and manage risks to safety, security, and trustworthiness arising from dual-use foundation models, building on guidelines issued pursuant to subsection 4.1(a) of Executive Order 14110. AISI shall issue guidance on topics including:

(A) How to measure capabilities that are relevant to the risk that AI models could enable the development of biological and chemical weapons or the automation of offensive cyber operations;

(B) How to address societal risks, such as the misuse of models to harass or impersonate individuals;

(C) How to develop mitigation measures to prevent malicious or improper use of models;

(D) How to test the efficacy of safety and security mitigations; and

(E) How to apply risk management practices throughout the development and deployment lifecycle (pre-development, development, and deployment/release).

(iii) Within 180 days of the date of this memorandum, AISI, in consultation with other agencies as appropriate, shall develop or recommend benchmarks or other methods for assessing AI systems' capabilities and limitations in science, mathematics, code generation, and general reasoning, as well as other categories of activity that AISI deems relevant to assessing general-purpose capabilities likely to have a bearing on national security and public safety.

(iv) In the event that AISI or another agency determines that a dual-use foundation model's capabilities could be used to harm public safety significantly, AISI shall serve

as the primary point of contact through which the United States Government communicates such findings and any associated recommendations regarding risk mitigation to the developer of the model.

(v) Within 270 days of the date of this memorandum, and at least annually thereafter, AISI shall submit to the President, through the APNSA, and provide to other interagency counterparts as appropriate, at minimum one report that shall include the following:

(A) A summary of findings from AI safety assessments of frontier AI models that have been conducted by or shared with AISI;

(B) A summary of whether AISI deemed risk mitigation necessary to resolve any issues identified in the assessments, along with conclusions regarding any mitigations' efficacy; and

(C) A summary of the adequacy of the science-based tools and methods used to inform such assessments.

(f) Consistent with these goals, other agencies specified below shall take the following actions, in coordination with Commerce, acting through AISI within NIST, to provide classified sector-specific evaluations of current and near-future AI systems for cyber, nuclear, and radiological risks:

(i) All agencies that conduct or fund safety testing and evaluations of AI systems shall share the results of such evaluations with AISI within 30 days of their completion, consistent with applicable protections for classified and controlled information.

(ii) Within 120 days of the date of this memorandum, the National Security Agency (NSA), acting through its AI Security Center (AISC) and in coordination with AISI, shall develop the capability to perform rapid systematic classified testing of AI models' capacity to detect, generate, and/or exacerbate offensive cyber threats. Such tests shall assess the degree to which AI systems, if misused, could accelerate offensive cyber operations.

(iii) Within 120 days of the date of this memorandum, DOE, acting primarily through the National Nuclear Security Administration (NNSA) and in close coordination with AISI and NSA, shall seek to develop the capability to perform rapid systematic testing of AI models' capacity to generate or exacerbate nuclear and radiological risks. This initiative shall involve the development and maintenance of infrastructure capable of running classified and unclassified tests, including using restricted data and relevant classified threat information. This initiative shall also feature the creation and regular updating of automated evaluations, the development of an interface for enabling human-led red-teaming, and the establishment of technical and legal tooling necessary for facilitating the rapid and secure transfer of United States Government, open-weight, and proprietary models to these facilities. As part of this initiative:

(A) Within 180 days of the date of this memorandum, DOE shall use the capability described in subsection 3.3(f)(iii) of this section to complete initial evaluations of the radiological and nuclear knowledge, capabilities, and implications of a frontier AI model no more than 30 days after the model has been made available to NNSA at an appropriate classification level. These evaluations shall involve tests of AI systems both without significant modifications and, as appropriate, with fine-tuning or other modifications that could enhance performance.

(B) Within 270 days of the date of this memorandum, and at least annually thereafter, DOE shall submit to the President, through the APNSA, at minimum one assessment that shall include the following:

- (1) A concise summary of the findings of each AI model evaluation for radiological and nuclear risk, described in subsection 3.3(f)(iii)(A) of this section, that DOE has performed in the preceding 12 months;
- (2) A recommendation as to whether corrective action is necessary to resolve any issues identified in the evaluations, including but not limited to actions necessary for attaining and sustaining compliance conditions appropriate to safeguard and prevent unauthorized disclosure of restricted data or other classified information, pursuant to the Atomic Energy Act of 1954; and
- (3) A concise statement regarding the adequacy of the science-based tools and methods used to inform the evaluations.

(iv) On an ongoing basis, DHS, acting through the Cybersecurity and Infrastructure Security Agency (CISA), shall continue to fulfill its responsibilities with respect to the application of AISI guidance, as identified in National Security Memorandum 22 of April 30, 2024 (Critical Infrastructure Security and Resilience), and section 4 of Executive Order 14110.

(g) Consistent with these goals, and to reduce the chemical and biological risks that could emerge from AI:

(i) The United States Government shall advance classified evaluations of advanced AI models' capacity to generate or exacerbate deliberate chemical and biological threats. As part of this initiative:

(A) Within 210 days of the date of this memorandum, DOE, DHS, and AISI, in consultation with DOD and other relevant agencies, shall coordinate to develop a roadmap for future classified evaluations of advanced AI models' capacity to generate or exacerbate deliberate chemical and biological threats, to be shared with the APNSA. This roadmap shall consider the scope, scale, and priority of classified evaluations; proper safeguards to ensure that evaluations and simulations are not misconstrued as offensive capability development; proper safeguards for testing sensitive and/or classified information; and sustainable implementation of evaluation methodologies.

(B) On an ongoing basis, DHS shall provide expertise, threat and risk information, and other technical support to assess the feasibility of proposed biological and chemical classified evaluations; interpret and contextualize evaluation results; and advise relevant agencies on potential risk mitigations.

(C) Within 270 days of the date of this memorandum, DOE shall establish a pilot project to provide expertise, infrastructure, and facilities capable of conducting classified tests in this area.

(ii) Within 240 days of the date of this memorandum, DOD, the Department of Health and Human Services (HHS), DOE (including national laboratories), DHS, NSF, and other agencies pursuing the development of AI systems substantially trained on biological and chemical data shall, as appropriate, support efforts to utilize high-performance computing resources and AI systems to enhance biosafety and biosecurity. These efforts shall include:

- (A) The development of tools for screening in silico chemical and biological research and technology;
- (B) The creation of algorithms for nucleic acid synthesis screening;
- (C) The construction of high-assurance software foundations for novel biotechnologies;
- (D) The screening of complete orders or data streams from cloud labs and biofoundries; and
- (E) The development of risk mitigation strategies such as medical countermeasures.

(iii) After the publication of biological and chemical safety guidance by AISI outlined in subsection 3.3(e) of this section, all agencies that directly develop relevant dual-use foundation AI models that are made available to the public and are substantially trained on biological or chemical data shall incorporate this guidance into their agency's practices, as appropriate and feasible.

(iv) Within 180 days of the date of this memorandum, NSF, in coordination with DOD, Commerce (acting through AISI within NIST), HHS, DOE, the Office of Science and Technology Policy (OSTP), and other relevant agencies, shall seek to convene academic research institutions and scientific publishers to develop voluntary best practices and standards for publishing computational biological and chemical models, data sets, and approaches, including those that use AI and that could contribute to the production of knowledge, information, technologies, and products that could be misused to cause harm. This is in furtherance of the activities described in subsections 4.4 and 4.7 of Executive Order 14110.

(v) Within 540 days of the date of this memorandum, and informed by the United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential, OSTP, NSC staff, and the Office of Pandemic Preparedness and Response Policy, in consultation with relevant agencies and external stakeholders as appropriate, shall develop guidance promoting the benefits of and mitigating the risks associated with in silico biological and chemical research.

(h) Agencies shall take the following actions to improve foundational understanding of AI safety, security, and trustworthiness:

(i) DOD, Commerce, DOE, DHS, ODNI, NSF, NSA, and the National Geospatial-Intelligence Agency (NGA) shall, as appropriate and consistent with applicable law, prioritize research on AI safety and trustworthiness. As appropriate and consistent with existing authorities, they shall pursue partnerships as appropriate with leading public sector, industry, civil society, academic, and other institutions with expertise in these domains, with the objective of accelerating technical and socio-technical progress in AI safety and trustworthiness. This work may include research on interpretability, formal methods, privacy enhancing technologies, techniques to address risks to civil liberties and human rights, human-AI interaction, and/or the socio-technical effects of detecting and labeling synthetic and authentic content (for example, to address the malicious use of AI to generate misleading videos or images, including those of a strategically damaging or non-consensual intimate nature, of political or public figures).

(ii) DOD, Commerce, DOE, DHS, ODNI, NSF, NSA, and NGA shall, as appropriate and consistent with applicable law, prioritize research to improve the security, robustness, and reliability of AI systems and controls. These entities shall, as

appropriate and consistent with applicable law, partner with other agencies, industry, civil society, and academia. Where appropriate, DOD, DHS (acting through CISA), the Federal Bureau of Investigation, and NSA (acting through AISC) shall publish unclassified guidance concerning known AI cybersecurity vulnerabilities and threats; best practices for avoiding, detecting, and mitigating such issues during model training and deployment; and the integration of AI into other software systems. This work shall include an examination of the role of and vulnerabilities potentially caused by AI systems used in critical infrastructure.

(i) Agencies shall take actions to protect classified and controlled information, given the potential risks posed by AI:

(i) In the course of regular updates to policies and procedures, DOD, DOE, and the IC shall consider how analysis enabled by AI tools may affect decisions related to declassification of material, standards for sufficient anonymization, and similar activities, as well as the robustness of existing operational security and equity controls to protect classified or controlled information, given that AI systems have demonstrated the capacity to extract previously inaccessible insight from redacted and anonymized data.

Sec. 4. Responsibly Harnessing AI to Achieve National Security Objectives. (a) It is the policy of the United States Government to act decisively to enable the effective and responsible use of AI in furtherance of its national security mission. Achieving global leadership in national security applications of AI will require effective partnership with organizations outside Government, as well as significant internal transformation, including strengthening effective oversight and governance functions.

4.1. Enabling Effective and Responsible Use of AI. (a) It is the policy of the United States Government to adapt its partnerships, policies, and infrastructure to use AI capabilities appropriately, effectively, and responsibly. These modifications must balance each agency's unique oversight, data, and application needs with the substantial benefits associated with sharing powerful AI and computational resources across the United States Government. Modifications must also be grounded in a clear understanding of the United States Government's comparative advantages relative to industry, civil society, and academia, and must leverage offerings from external collaborators and contractors as appropriate. The United States Government must make the most of the rich United States AI ecosystem by incentivizing innovation in safe, secure, and trustworthy AI and promoting industry competition when selecting contractors, grant recipients, and research collaborators. Finally, the United States Government must address important technical and policy considerations in ways that ensure the integrity and interoperability needed to pursue its objectives while protecting human rights, civil rights, civil liberties, privacy, and safety.

(b) The United States Government needs an updated set of Government-wide procedures for attracting, hiring, developing, and retaining AI and AI-enabling talent for national security purposes.

(c) Consistent with these goals:

(i) In the course of regular legal, policy, and compliance framework reviews, the Department of State, DOD, DOJ, DOE, DHS, and IC elements shall revise, as appropriate, their hiring and retention policies and strategies to accelerate responsible AI adoption. Agencies shall account for technical talent needs required to adopt AI and integrate it into their missions and other roles necessary to use AI effectively, such as AI-related governance, ethics, and policy positions. These policies and strategies shall

identify financial, organizational, and security hurdles, as well as potential mitigations consistent with applicable law. Such measures shall also include consideration of programs to attract experts with relevant technical expertise from industry, academia, and civil society—including scholarship for service programs—and similar initiatives that would expose Government employees to relevant non-government entities in ways that build technical, organizational, and cultural familiarity with the AI industry. These policies and strategies shall use all available authorities, including expedited security clearance procedures as appropriate, in order to address the shortfall of AI-relevant talent within Government.

(ii) Within 120 days of the date of this memorandum, the Department of State, DOD, DOJ, DOE, DHS, and IC elements shall each, in consultation with the Office of Management and Budget (OMB), identify education and training opportunities to increase the AI competencies of their respective workforces, via initiatives which may include training and skills-based hiring.

(d) To accelerate the use of AI in service of its national security mission, the United States Government needs coordinated and effective acquisition and procurement systems. This will require an enhanced capacity to assess, define, and articulate AI-related requirements for national security purposes, as well as improved accessibility for AI companies that lack significant prior experience working with the United States Government.

(e) Consistent with these goals:

(i) Within 30 days of the date of this memorandum, DOD and ODNI, in coordination with OMB and other agencies as appropriate, shall establish a working group to address issues involving procurement of AI by DOD and IC elements and for use on NSS. As appropriate, the working group shall consult the Director of the NSA, as the National Manager for NSS, in developing recommendations for acquiring and procuring AI for use on NSS.

(ii) Within 210 days of the date of this memorandum, the working group described in subsection 4.1(e)(i) of this section shall provide written recommendations to the Federal Acquisition Regulatory Council (FARC) regarding changes to existing regulations and guidance, as appropriate and consistent with applicable law, to promote the following objectives for AI procured by DOD and IC elements and for use on NSS:

(A) Ensuring objective metrics to measure and promote the safety, security, and trustworthiness of AI systems;

(B) Accelerating the acquisition and procurement process for AI, consistent with the Federal Acquisition Regulation, while maintaining appropriate checks to mitigate safety risks;

(C) Simplifying processes such that companies without experienced contracting teams may meaningfully compete for relevant contracts, to ensure that the United States Government has access to a wide range of AI systems and that the AI marketplace is competitive;

(D) Structuring competitions to encourage robust participation and achieve best value to the Government, such as by including requirements that promote interoperability and prioritizing the technical capability of vendors when evaluating offers;

(E) Accommodating shared use of AI to the greatest degree possible and as appropriate across relevant agencies; and

(F) Ensuring that agencies with specific authorities and missions may implement other policies, where appropriate and necessary.

(iii) The FARC shall, as appropriate and consistent with applicable law, consider proposing amendments to the Federal Acquisition Regulation to codify recommendations provided by the working group pursuant to subsection 4.1(e)(ii) of this section that may have Government-wide application.

(iv) DOD and ODNI shall seek to engage on an ongoing basis with diverse United States private sector stakeholders—including AI technology and defense companies and members of the United States investor community—to identify and better understand emerging capabilities that would benefit or otherwise affect the United States national security mission.

(f) The United States Government needs clear, modernized, and robust policies and procedures that enable the rapid development and national security use of AI, consistent with human rights, civil rights, civil liberties, privacy, safety, and other democratic values.

(g) Consistent with these goals:

(i) DOD and the IC shall, in consultation with DOJ as appropriate, review their respective legal, policy, civil liberties, privacy, and compliance frameworks, including international legal obligations, and, as appropriate and consistent with applicable law, seek to develop or revise policies and procedures to enable the effective and responsible use of AI, accounting for the following:

(A) Issues raised by the acquisition, use, retention, dissemination, and disposal of models trained on datasets that include personal information traceable to specific United States persons, publicly available information, commercially available information, and intellectual property, consistent with section 9 of Executive Order 14110;

(B) Guidance that shall be developed by DOJ, in consultation with DOD and ODNI, regarding constitutional considerations raised by the IC's acquisition and use of AI;

(C) Challenges associated with classification and compartmentalization;

(D) Algorithmic bias, inconsistent performance, inaccurate outputs, and other known AI failure modes;

(E) Threats to analytic integrity when employing AI tools;

(F) Risks posed by a lack of safeguards that protect human rights, civil rights, civil liberties, privacy, and other democratic values, as addressed in further detail in subsection 4.2 of this section;

(G) Barriers to sharing AI models and related insights with allies and partners; and

(H) Potential inconsistencies between AI use and the implementation of international legal obligations and commitments.

(ii) As appropriate, the policies described in subsection 4.1(g) of this section shall be consistent with direction issued by the Committee on NSS and DOD governing the security of AI used on NSS, policies issued by the Director of National Intelligence governing adoption of AI by the IC, and direction issued by OMB governing the security of AI used on non-NSS.

(iii) On an ongoing basis, each agency that uses AI on NSS shall, in consultation with ODNI and DOD, take all steps appropriate and consistent with applicable law to accelerate responsible approval of AI systems for use on NSS and accreditation of NSS that use AI systems.

(h) The United States' network of allies and partners confers significant advantages over competitors. Consistent with the 2022 National Security Strategy or any successor strategies, the United States Government must invest in and proactively enable the co-development and co-deployment of AI capabilities with select allies and partners.

(i) Consistent with these goals:

(i) Within 150 days of the date of this memorandum, DOD, in coordination with the Department of State and ODNI, shall evaluate the feasibility of advancing, increasing, and promoting co-development and shared use of AI and AI-enabled assets with select allies and partners. This evaluation shall include:

(A) A potential list of foreign states with which such co-development or co-deployment may be feasible;

(B) A list of bilateral and multilateral fora for potential outreach;

(C) Potential co-development and co-deployment concepts;

(D) Proposed classification-appropriate testing vehicles for co-developed AI capabilities; and

(E) Considerations for existing programs, agreements, or arrangements to use as foundations for future co-development and co-deployment of AI capabilities.

(j) The United States Government needs improved internal coordination with respect to its use of and approach to AI on NSS in order to ensure interoperability and resource sharing consistent with applicable law, and to reap the generality and economies of scale offered by frontier AI models.

(k) Consistent with these goals:

(i) On an ongoing basis, DOD and ODNI shall issue or revise relevant guidance to improve consolidation and interoperability across AI functions on NSS. This guidance shall seek to ensure that the United States Government can coordinate and share AI-related resources effectively, as appropriate and consistent with applicable law. Such work shall include:

(A) Recommending agency organizational practices to improve AI research and deployment activities that span multiple national security institutions. In order to encourage AI adoption for the purpose of national security, these measures shall aim to create consistency to the greatest extent possible across the revised practices.

(B) Steps that enable consolidated research, development, and procurement for general-purpose AI systems and supporting infrastructure, such that multiple agencies can share access to these tools to the extent consistent with applicable law, while still allowing for appropriate controls on sensitive data.

(C) Aligning AI-related national security policies and procedures across agencies, as practicable and appropriate, and consistent with applicable law.

(D) Developing policies and procedures, as appropriate and consistent with applicable law, to share information across DOD and the IC when an AI system

developed, deployed, or used by a contractor demonstrates risks related to safety, security, and trustworthiness, including to human rights, civil rights, civil liberties, or privacy.

4.2. Strengthening AI Governance and Risk Management. (a) As the United States Government moves swiftly to adopt AI in support of its national security mission, it must continue taking active steps to uphold human rights, civil rights, civil liberties, privacy, and safety; ensure that AI is used in a manner consistent with the President's authority as Commander in Chief to decide when to order military operations in the Nation's defense; and ensure that military use of AI capabilities is accountable, including through such use during military operations within a responsible human chain of command and control. Accordingly, the United States Government must develop and implement robust AI governance and risk management practices to ensure that its AI innovation aligns with democratic values, updating policy guidance where necessary. In light of the diverse authorities and missions across covered agencies with a national security mission and the rapid rate of ongoing technological change, such AI governance and risk management frameworks shall be:

- (i) Structured, to the extent permitted by law, such that they can adapt to future opportunities and risks posed by new technical developments;
- (ii) As consistent across agencies as is practicable and appropriate in order to enable interoperability, while respecting unique authorities and missions;
- (iii) Designed to enable innovation that advances United States national security objectives;
- (iv) As transparent to the public as practicable and appropriate, while protecting classified or controlled information;
- (v) Developed and applied in a manner and with means to integrate protections, controls, and safeguards for human rights, civil rights, civil liberties, privacy, and safety where relevant; and
- (vi) Designed to reflect United States leadership in establishing broad international support for rules and norms that reinforce the United States' approach to AI governance and risk management.

(b) Covered agencies shall develop and use AI responsibly, consistent with United States law and policies, democratic values, and international law and treaty obligations, including international humanitarian and human rights law. All agency officials retain their existing authorities and responsibilities established in other laws and policies.

(c) Consistent with these goals:

- (i) Heads of covered agencies shall, consistent with their authorities, monitor, assess, and mitigate risks directly tied to their agency's development and use of AI. Such risks may result from reliance on AI outputs to inform, influence, decide, or execute agency decisions or actions, when used in a defense, intelligence, or law enforcement context, and may impact human rights, civil rights, civil liberties, privacy, safety, national security, and democratic values. These risks from the use of AI include the following:
 - (A) Risks to physical safety: AI use may pose unintended risks to human life or property.
 - (B) Privacy harms: AI design, development, and operation may result in harm, embarrassment, unfairness, and prejudice to individuals.

(C) Discrimination and bias: AI use may lead to unlawful discrimination and harmful bias, resulting in, for instance, inappropriate surveillance and profiling, among other harms.

(D) Inappropriate use: operators using AI systems may not fully understand the capabilities and limitations of these technologies, including systems used in conflicts. Such unfamiliarity could impact operators' ability to exercise appropriate levels of human judgment.

(E) Lack of transparency: agencies may have gaps in documentation of AI development and use, and the public may lack access to information about how AI is used in national security contexts because of the necessity to protect classified or controlled information.

(F) Lack of accountability: training programs and guidance for agency personnel on the proper use of AI systems may not be sufficient, including to mitigate the risk of overreliance on AI systems (such as "automation bias"), and accountability mechanisms may not adequately address possible intentional or negligent misuse of AI-enabled technologies.

(G) Data spillage: AI systems may reveal aspects of their training data—either inadvertently or through deliberate manipulation by malicious actors—and data spillage may result from AI systems trained on classified or controlled information when used on networks where such information is not permitted.

(H) Poor performance: AI systems that are inappropriately or insufficiently trained, used for purposes outside the scope of their training set, or improperly integrated into human workflows may exhibit poor performance, including in ways that result in inconsistent outcomes or unlawful discrimination and harmful bias, or that undermine the integrity of decision-making processes.

(I) Deliberate manipulation and misuse: foreign state competitors and malicious actors may deliberately undermine the accuracy and efficacy of AI systems, or seek to extract sensitive information from such systems.

(d) The United States Government's AI governance and risk management policies must keep pace with evolving technology.

(e) Consistent with these goals:

(i) An AI framework, entitled "Framework to Advance AI Governance and Risk Management in National Security" (AI Framework), shall further implement this subsection. The AI Framework shall be approved by the NSC Deputies Committee through the process described in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), or any successor process, and shall be reviewed periodically through that process. This process shall determine whether adjustments are needed to address risks identified in subsection 4.2(c) of this section and other topics covered in the AI Framework. The AI Framework shall serve as a national security-focused counterpart to OMB's Memorandum M–24–10 of March 28, 2024 (Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence), and any successor OMB policies. To the extent feasible, appropriate, and consistent with applicable law, the AI Framework shall be as consistent as possible with these OMB policies and shall be made public.

(ii) The AI Framework described in subsection 4.2(e)(i) of this section and any successor document shall, at a minimum, and to the extent consistent with applicable law, specify the following:

- (A) Each covered agency shall have a Chief AI Officer who holds primary responsibility within that agency, in coordination with other responsible officials, for managing the agency's use of AI, promoting AI innovation within the agency, and managing risks from the agency's use of AI consistent with subsection 3(b) of OMB Memorandum M-24-10, as practicable.
- (B) Covered agencies shall have AI Governance Boards to coordinate and govern AI issues through relevant senior leaders from the agency.
- (C) Guidance on AI activities that pose unacceptable levels of risk and that shall be prohibited.
- (D) Guidance on AI activities that are "high impact" and require minimum risk management practices, including for high-impact AI use that affects United States Government personnel. Such high-impact activities shall include AI whose output serves as a principal basis for a decision or action that could exacerbate or create significant risks to national security, international norms, human rights, civil rights, civil liberties, privacy, safety, or other democratic values. The minimum risk management practices for high-impact AI shall include a mechanism for agencies to assess AI's expected benefits and potential risks; a mechanism for assessing data quality; sufficient test and evaluation practices; mitigation of unlawful discrimination and harmful bias; human training, assessment, and oversight requirements; ongoing monitoring; and additional safeguards for military service members, the Federal civilian workforce, and individuals who receive an offer of employment from a covered agency.
- (E) Covered agencies shall ensure privacy, civil liberties, and safety officials are integrated into AI governance and oversight structures. Such officials shall report findings to the heads of agencies and oversight officials, as appropriate, using existing reporting channels when feasible.
- (F) Covered agencies shall ensure that there are sufficient training programs, guidance, and accountability processes to enable proper use of AI systems.
- (G) Covered agencies shall maintain an annual inventory of their high-impact AI use and AI systems and provide updates on this inventory to agency heads and the APNSA.
- (H) Covered agencies shall ensure that whistleblower protections are sufficient to account for issues that may arise in the development and use of AI and AI systems.
- (I) Covered agencies shall develop and implement waiver processes for high-impact AI use that balance robust implementation of risk mitigation measures in this memorandum and the AI Framework with the need to utilize AI to preserve and advance critical agency missions and operations.
- (J) Covered agencies shall implement cybersecurity guidance or direction associated with AI systems issued by the National Manager for NSS to mitigate the risks posed by malicious actors exploiting new technologies, and to enable interoperability of AI across agencies. Within 150 days of the date of this memorandum, and periodically thereafter, the National Manager for NSS shall issue minimum cybersecurity guidance and/or direction for AI used as a

component of NSS, which shall be incorporated into AI governance guidance detailed in subsection 4.2(g)(i) of this section.

(f) The United States Government needs guidance specifically regarding the use of AI on NSS.

(g) Consistent with these goals:

(i) Within 180 days of the date of this memorandum, the heads of the Department of State, the Department of the Treasury, DOD, DOJ, Commerce, DOE, DHS, ODNI (acting on behalf of the 18 IC elements), and any other covered agency that uses AI as part of a NSS (Department Heads) shall issue or update guidance to their components/sub-agencies on AI governance and risk management for NSS, aligning with the policies in this subsection, the AI Framework, and other applicable policies. Department Heads shall review their respective guidance on an annual basis, and update such guidance as needed. This guidance, and any updates thereto, shall be provided to the APNSA prior to issuance. This guidance shall be unclassified and made available to the public to the extent feasible and appropriate, though it may have a classified annex. Department Heads shall seek to harmonize their guidance, and the APNSA shall convene an interagency meeting at least annually for the purpose of harmonizing Department Heads' guidance on AI governance and risk management to the extent practicable and appropriate while respecting the agencies' diverse authorities and missions. Harmonization shall be pursued in the following areas:

(A) Implementation of the risk management practices for high-impact AI;

(B) AI and AI system standards and activities, including as they relate to training, testing, accreditation, and security and cybersecurity; and

(C) Any other issues that affect interoperability for AI and AI systems.

Sec. 5. Fostering a Stable, Responsible, and Globally Beneficial International AI Governance Landscape. (a) Throughout its history, the United States has played an essential role in shaping the international order to enable the safe, secure, and trustworthy global adoption of new technologies while also protecting democratic values. These contributions have ranged from establishing nonproliferation regimes for biological, chemical, and nuclear weapons to setting the foundations for multi-stakeholder governance of the Internet. Like these precedents, AI will require new global norms and coordination mechanisms, which the United States Government must maintain an active role in crafting.

(b) It is the policy of the United States Government that United States international engagement on AI shall support and facilitate improvements to the safety, security, and trustworthiness of AI systems worldwide; promote democratic values, including respect for human rights, civil rights, civil liberties, privacy, and safety; prevent the misuse of AI in national security contexts; and promote equitable access to AI's benefits. The United States Government shall advance international agreements, collaborations, and other substantive and norm-setting initiatives in alignment with this policy.

(c) Consistent with these goals:

(i) Within 120 days of the date of this memorandum, the Department of State, in coordination with DOD, Commerce, DHS, the United States Mission to the United Nations (USUN), and the United States Agency for International Development (USAID), shall produce a strategy for the advancement of international AI governance norms in line with safe, secure, and trustworthy AI, and democratic values, including human rights, civil rights, civil liberties, and privacy. This strategy shall cover bilateral

and multilateral engagement and relations with allies and partners. It shall also include guidance on engaging with competitors, and it shall outline an approach to working in international institutions such as the United Nations and the Group of 7 (G7), as well as technical organizations. The strategy shall:

(A) Develop and promote internationally shared definitions, norms, expectations, and standards, consistent with United States policy and existing efforts, which will promote safe, secure, and trustworthy AI development and use around the world. These norms shall be as consistent as possible with United States domestic AI governance (including Executive Order 14110 and OMB Memorandum M-24-10), the International Code of Conduct for Organizations Developing Advanced AI Systems released by the G7 in October 2023, the Organization for Economic Cooperation and Development Principles on AI, United Nations General Assembly Resolution A/78/L.49, and other United States-supported relevant international frameworks (such as the Political Declaration on Responsible Military Use of AI and Autonomy) and instruments. By discouraging misuse and encouraging appropriate safeguards, these norms and standards shall aim to reduce the likelihood of AI causing harm or having adverse impacts on human rights, democracy, or the rule of law.

(B) Promote the responsible and ethical use of AI in national security contexts in accordance with democratic values and in compliance with applicable international law. The strategy shall advance the norms and practices established by this memorandum and measures endorsed in the Political Declaration on Responsible Military Use of AI and Autonomy.

Sec. 6. Ensuring Effective Coordination, Execution, and Reporting of AI Policy. (a) The United States Government must work in a closely coordinated manner to make progress on effective and responsible AI adoption. Given the speed with which AI technology evolves, the United States Government must learn quickly, adapt to emerging strategic developments, adopt new capabilities, and confront novel risks.

(b) Consistent with these goals:

(i) Within 270 days of the date of this memorandum, and annually thereafter for at least the next 5 years, the heads of the Department of State, DOD, Commerce, DOE, ODNI (acting on behalf of the IC), USUN, and USAID shall each submit a report to the President, through the APNSA, that offers a detailed accounting of their activities in response to their taskings in all sections of this memorandum, including this memorandum's classified annex, and that provides a plan for further action. The Central Intelligence Agency (CIA), NSA, the Defense Intelligence Agency (DIA), and NGA shall submit reports on their activities to ODNI for inclusion in full as an appendix to ODNI's report regarding IC activities. NGA, NSA, and DIA shall submit their reports as well to DOD for inclusion in full as an appendix to DOD's report.

(ii) Within 45 days of the date of this memorandum, the Chief AI Officers of the Department of State, DOD, DOJ, DOE, DHS, OMB, ODNI, CIA, DIA, NSA, and NGA, as well as appropriate technical staff, shall form an AI National Security Coordination Group (Coordination Group). Any Chief AI Officer of an agency that is a member of the Committee on National Security Systems may also join the Coordination Group as a full member. The Coordination Group shall be co-chaired by the Chief AI Officers of ODNI and DOD. The Coordination Group shall consider ways to harmonize policies relating to the development, accreditation, acquisition, use, and evaluation of AI on NSS. This work could include development of:

- (A) Enhanced training and awareness to ensure that agencies prioritize the most effective AI systems, responsibly develop and use AI, and effectively evaluate AI systems;
- (B) Best practices to identify and mitigate foreign intelligence risks and human rights considerations associated with AI procurement;
- (C) Best practices to ensure interoperability between agency deployments of AI, to include data interoperability and data sharing agreements, as appropriate and consistent with applicable law;
- (D) A process to maintain, update, and disseminate such trainings and best practices on an ongoing basis;
- (E) AI-related policy initiatives to address regulatory gaps implicated by executive branch-wide policy development processes; and
- (F) An agile process to increase the speed of acquisitions, validation, and delivery of AI capabilities, consistent with applicable law.

(iii) Within 90 days of the date of this memorandum, the Coordination Group described in subsection (b)(ii) of this section shall establish a National Security AI Executive Talent Committee (Talent Committee) composed of senior AI officials (or designees) from all agencies in the Coordination Group that wish to participate. The Talent Committee shall work to standardize, prioritize, and address AI talent needs and develop an updated set of Government-wide procedures for attracting, hiring, developing, and retaining AI and AI-enabling talent for national security purposes. The Talent Committee shall designate a representative to serve as a member of the AI and Technology Talent Task Force set forth in Executive Order 14110, helping to identify overlapping needs and address shared challenges in hiring.

(iv) Within 365 days of the date of this memorandum, and annually thereafter for at least the next 5 years, the Coordination Group described in subsection (b)(ii) of this section shall issue a joint report to the APNSA on consolidation and interoperability of AI efforts and systems for the purposes of national security.

Sec. 7. Definitions. (a) This memorandum uses definitions set forth in section 3 of Executive Order 14110. In addition, for the purposes of this memorandum:

- (i) The term "AI safety" means the mechanisms through which individuals and organizations minimize and mitigate the potential for harm to individuals and society that can result from the malicious use, misapplication, failures, accidents, and unintended behavior of AI models; the systems that integrate them; and the ways in which they are used.
- (ii) The term "AI security" means a set of practices to protect AI systems—including training data, models, abilities, and lifecycles—from cyber and physical attacks, thefts, and damage.
- (iii) The term "covered agencies" means agencies in the Intelligence Community, as well as all agencies as defined in 44 U.S.C. 3502(1) when they use AI as a component of a National Security System, other than the Executive Office of the President.
- (iv) The term "Critical Technical Artifacts" (CTAs) means information, usually specific to a single model or group of related models that, if possessed by someone other than the model developer, would substantially lower the costs of recreating, attaining, or using the model's capabilities. Under the technical paradigm dominant in the AI

industry today, the model weights of a trained AI system constitute CTAs, as do, in some cases, associated training data and code. Future paradigms may rely on different CTAs.

(v) The term "frontier AI model" means a general-purpose AI system near the cutting-edge of performance, as measured by widely accepted publicly available benchmarks, or similar assessments of reasoning, science, and overall capabilities.

(vi) The term "Intelligence Community" (IC) has the meaning provided in 50 U.S.C. 3003.

(vii) The term "open-weight model" means a model that has weights that are widely available, typically through public release.

(viii) The term "United States Government" means all agencies as defined in 44 U.S.C. 3502(1).

Sec. 8. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

NOTE: An original was not available for verification of the content of this memorandum.

Categories: Communications to Federal Agencies : Artificial intelligence, efforts to advance U.S. leadership, fulfill national security objectives, and foster safety, security, and trustworthiness, memorandum.

Subjects: Artificial intelligence and other emerging technologies; Civil and human rights, U.S. promotion efforts; Climate change; Committee on Foreign Investment in the U.S.; Council of Economic Advisers; Cybersecurity and Infrastructure Security Agency; Cybersecurity, strengthening efforts; Intelligence gathering; National Economic Council; National Science Foundation; National Security Adviser; National security, artificial intelligence impacts; Privacy; Research and development; White House Chief of Staff.

DCPD Number: DCPD202400945.