NSF, OSTP, and NITRD NCO Request for Information:
Development of an Artificial Intelligence (AI) Action Plan

MERCYHURST
—UNIVERSITY—

On Behalf Of:

Center for Intelligence, Research, Analysis, and Training (CIRAT)
Mercyhurst University
501 E. 38th St.
Erie, PA 16546

Contact Information

Brian Fuller, CIRAT Executive Director
Office Phone: (814) [redacted]
Email: [redacted]

Contributors:

Brian Fuller
CIRAT Executive Director

Jay Dalmaso
CIRAT Graduate Assistant

Gianfranco Machado-Lopez
CIRAT Graduate Assistant

Brandon T. Mazzei
CIRAT Graduate Assistant

Zachary T. Prisk
CIRAT Graduate Assistant

Anthony Soltis
CIRAT Cybersecurity Team Leader

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

Contents

Executive Summary

Artificial Intelligence (AI) is a rapidly evolving technology that is likely to grow at a pace faster than policy can keep up. In this document, the Center for Intelligence Research, Analysis, and Training (CIRAT) has outlined ways in which policy can stay ahead of the curve and implement strategies that will keep the U.S. innovative, competitive, and safe. We have proposed key policy recommendations in 16 areas ranging from Cyber & National Security, Manufacturing & Supply Chain, Development & Regulation, and Innovation & Competition.

Key Policy Recommendations

The following policy recommendations are deemed essential to ensure that the U.S. maintains its leadership and advances in the field of AI:

- Create an open-source AI training network that will allow independent researchers, academic institutions, and start-ups to research and develop AI models.
- Create an open-source AI-driven public funding assistant for independent researchers, academic institutions, and start-ups to identify grant and funding opportunities.
- Develop a decentralized AI compute marketplace for independent researchers, academic institutions, and start-ups to reduce reliance on large tech firms.
- Develop an ethical AI-driven auditing system to ensure ethical compliance and transparency standards.
- To ensure that new entrants can become competitive and add meaningful innovation to the AI market, it is recommended that more robust antitrust enforcement be implemented in the AI industry.
- To ensure that intellectual property (IP) enforcement is fair and does not overreach or contribute to false takedowns, human oversight and regulation must be implemented regarding the relationship between AI and the IP law industry.
- To ensure AI is protected, the use of AI models and technologies that may be used for national security is restricted.
- Ensure freedom of navigation in the seas to promote free trade and open supply chains for chips by building international consensus and expanding regional partnerships.
- Increase the economic and financial incentives for chip manufacturers to open advanced chip fabrication facilities in the U.S. to increase domestic chip fabrication.
- Increase domestic energy production and infrastructure in strategic economic corridors for data centers and/or chip fabrication facilities due to increased energy demands.
- Enhance security in semiconductor design and AI accelerators to prevent adversarial exploitation.
- Strengthening AI data center security to mitigate cyber threats and protect AI workloads.
- Ensure AI security throughout the deployment pipeline.
- Develop AI safety and cybersecurity standards to ensure trustworthiness.
- Enhance AI applications for cybersecurity, intelligence, and military operations.

- Establish comprehensive AI regulations and frameworks to ensure responsible development, deployment, and use while balancing innovation and risk mitigation.
- Develop regulations and frameworks; entities such as the National Institute of Standards and Technology (NIST) should be consulted and utilized, building upon existing frameworks and expanding them to address emerging AI challenges.
- Maintain international collaboration.
- Ensure compliance with data regulation standards.
- Transparency and accountability should be encouraged and enforced throughout the development of AI models.
- Establish standardized safety testing to ensure that AI development is safe before public use.
- Leverage privacy-preserving AI techniques that are essential for secure data processing.

Development and Implementation Strategies

- **Creating an open-source AI training network will allow independent researchers, academic institutions, and start-ups to research and develop AI models.** An open-source framework would offer pre-trained models, high-quality datasets, and shared computing resources to independent researchers, academic institutions, and start-ups to research and develop AI models. A practical application of this initiative would be a small AI start-up leveraging open-source resources to create an advanced medical diagnostic tool (Brynjolfsson & McAfee, 2023).

- **Create an open-source AI-driven public funding assistant for independent researchers, academic institutions, and start-ups to identify grant and funding opportunities**. The open-source AI-driven public funding assistant will use machine learning algorithms to analyze funding opportunities and match them with applicants based on their project scope, technical requirements, and financial needs (European Commission, 2024). For instance, a researcher working on AI-driven climate modeling could use the funding assistant to locate and secure grants, thereby accelerating project implementation and reducing the financial strain associated with AI development (OECD, 2024)**.**

- **Develop a decentralized AI compute marketplace for independent researchers, academic institutions, and start-ups to reduce reliance on large tech firms**. A decentralized AI compute marketplace utilizing blockchain technology will reduce reliance on large tech firms for computing resources (Feldman, Martin, & Skop, 2024). This marketplace would allow businesses and researchers to access distributed GPU resources competitively, breaking the dependence on cloud computing providers. In practice, a start-up requiring high-performance computing resources for AI training could lease GPU power from independent providers at a fraction of the cost, significantly lowering operational expenses and increasing accessibility to AI infrastructure (Mitchell, 2023).

- **Develop an ethical AI-driven auditing system to ensure ethical compliance and transparency standards.** Implementing an ethical AI-driven auditing system would ensure that AI applications adhere to fairness and transparency standards before deployment. This system would employ AI-driven regulatory tools to audit machine learning models for biases, unethical decision-making, and discriminatory practices (OECD, 2024). A practical use case would be a financial institution integrating this auditing system into its loan approval AI model to ensure that it does not discriminate against specific demographic groups, fostering trust and compliance with legal and ethical guidelines (Korinek & Vipra, 2025).

Minimizing AI Monopolies

- **To ensure that new entrants can become competitive and add meaningful innovation to the AI market, it is recommended that more robust antitrust enforcement be implemented in the AI industry.** Advancement in artificial intelligence is crucial in the digital age, but it should prioritize equitable competition. The average cost varies widely based on the organization's AI needs, with small-scale AI automation starting at around $10,000 and enterprise-grade projects reaching $1 million or more (Trotolo, Hayat, & Hayat, 2025). Cost is undeniably a significant barrier to entry into the AI market, and it is not likely to ease. For example, Epoch researchers estimate that training Google's DeepMind Gemini model costs $650 million, and they predict that the expenses for developing similar AI models will double every six months (Korinek & Vipra, 2025). Due to the high cost being a barrier to entry and most larger tech companies owning multiple parts of the supply chain, the AI market is vertically integrated and monopolized (Korinek & Vipra, 2025). The policy could include limiting the self-preferencing of existing AI companies and guaranteeing fair pricing for AI infrastructure. Further, by increasing public funding through grants, tax incentives, or incubators, barriers to entry could be lowered for new developers and researchers. This policy can be rolled out in three stages: First, inviting the current most significant market share owners to bring their opinions and solutions to a public forum to discuss mitigation strategies and the way ahead. Second, public policy can be drafted based on industry and NSF recommendations. Third, a complete and swift policy rollout with enforcement begins immediately.

Human Oversight in AI's Use During IP Enforcement

- **To ensure that IP enforcement is fair and does not overreach or contribute to false takedowns, human oversight, and regulation must be implemented regarding the relationship between AI and the IP law industry.** Due to the rapid development of AI tools and assistants across the industry, most organizations likely have someone in their office using AI. This widespread use leads to undue exposure for anyone using AI-generated work for a commercial product (Godefroy, 2024). AI can help mitigate IP theft and enforce transnational laws, but it faces several challenges. Given the complexities of IP and the current limitations of AI, it is primarily capable of tracking and monitoring. Humans must review the insights generated by AI to ensure accuracy and correct errors (Suwanmatajarn, 2024). Policy considerations should involve identifying any legal cases that utilized AI, allowing for further review to ensure no errors exist in those cases. Additionally, by adding human controls to the review process before takedowns or cease-and-desist orders, organizations can rest assured that there is no counter-case option

based on a frivolous or false takedown. This policy could first be implemented at the federal district court level to identify and resolve issues before being expanded to other levels.

Expanding AI Export Regulation

- **To ensure AI is protected, the use of AI models and technologies that may be used for national security is restricted.** The United States must continue adapting export controls on chips and critical AI models to keep them from adversaries while continuing to enable access for trusted partners (Bureau of Industry and Security [BIS], 2025). Future AI policy should strengthen international cooperation to balance AI export controls and prevent evasion. (BIS, 2025) The Department of Commerce's Bureau of Industry and Security (BIS) should utilize existing "catch-all" controls to restrict AI exports. (Weinstein & Wolf, 2023) The U.S. should enforce and consider expanding individual sanction controls to prevent supporting activities detrimental to national security (Weinstein & Wolf, 2023). The U.S. needs to be dynamic in its definitions and technical thresholds for AI export controls to ensure effective implementation due to the evolving technology (Plotinsky, 2024). For example, the Biden-Harris administration placed specific export controls on chips and certain AI models through the BIS (Bureau of Industry and Security, 2025). This new regulatory framework, announced on 13 January 2025, requires authorizations to export, reexport, and transfer these items to a broad list of countries (BIS, 2025). As a result, a company now needs to obtain a license to export high-performance AI training infrastructure to a country on the list (BIS, 2025). New AI export controls can be implemented as AI evolves and new technologies needing protection are developed.

Supply Chain Stability

- **Ensure freedom of navigation in the seas to promote free trade and open supply chains for chips by building international consensus and expanding regional partnerships.** Until the U.S. increases domestic chip production, it must ensure freedom of navigation at sea to promote free chip trade, as U.S. firms represent 10-12 percent of global chip manufacturing (SIA, 2020). Taiwan (25.4 percent), South Korea (18.3 percent), China (14.8 percent), and Japan (13 percent) account for 71.5 percent of global chip manufacturing, making the Indo-Pacific region the epicenter of chip manufacturing (Thadani & Allen, 2023). As geopolitical tensions rise between the U.S. and China in the Indo-Pacific, China increases its maritime presence and aggression in the South China Sea and the broader Indo-Pacific (CFR, 2024). China uses its Coast Guard and civilian vessels to conduct gray zone operations to intimidate its neighbors while disrupting economic activity in the Indo-Pacific region (Helmus et al., 2024).

Hardware and Chip Manufacturing

- **Increase the economic and financial incentives for chip manufacturers to open advanced chip fabrication facilities in the U.S. to increase domestic chip fabrication.** The U.S. and its state governments can create financial incentives by increasing access to financial capital, extending tax credits, and increasing grant opportunities (Burner, 2023; Zhai, 2024). The U.S. and its state governments can leverage existing tax credits, including the Advanced Manufacturing Incentive Credit and various state tax credits, to promote domestic chip manufacturing (Rojas, 2024). State and/or local governments can

promote public-private partnerships by creating state and/or local commissions, offering land-lease agreements to chip manufacturers, and expanding educational opportunities to local communities to build an employment pipeline (NCSL, 2017; Investopedia, 2024). For example, Intel's *Silicon Heartland* project in New Albany, Ohio, includes $28 billion in total private investment, including $100 million in K-12 and institutions of higher education in Ohio (Intel, 2024). The Ohio Department of Transportation (ODOT) invests $90 million to improve transportation infrastructure near the New Albany industrial park (Silicon Heartland, 2025).

Energy Consumption and Efficiency

- **Increase domestic energy production and infrastructure in strategic economic corridors for data centers and/or chip fabrication facilities due to increased energy demands.** The U.S. and its state governments must increase energy production and infrastructure to account for the increased energy demand of data centers and chip fabrication facilities (Spencer & Singh, 2024). AI Data centers currently account for one to two percent of global energy consumption; by 2030, they are expected to represent 21 percent (Stackpole, 2025). xAI's "Colossus" facility in Memphis, Tennessee, the largest data center globally, requires 250 MWs for 200,000 GPUs, with its next expansion to include one million GPUs, requiring nearly 1,000 MWs to operate (Smith, 2024; Allen, 2025).

Hardware and Chip Cybersecurity

- **Enhance security in semiconductor design and AI accelerators to prevent adversarial exploitation.** As AI workloads rely on specialized chips such as GPUs, TPUs, and neuromorphic processors, securing semiconductor hardware is critical to mitigating cyber risks. Implement security-by-design principles for AI chips using *NIST's Platform Firmware Resiliency Guidelines* to protect against firmware attacks (National Institute of Standards and Technology [NIST], 2018). Tamper-resistant AI hardware is required following *ISO/IEC 27001 Information Security Management*, ensuring chip-level protection against side-channel attacks and reverse engineering (ISO, 2022). Develop federal AI hardware security standards aligned with *DOD's Trusted Foundry Program*, ensuring secure fabrication of AI-optimized processors for defense and critical infrastructure applications (DOD, 2024). Enhance the security monitoring of the AI chip supply chain by utilizing CISA's Secure Hardware Development Framework to identify compromised components before deployment (NIST, 2024).

Data Center Cybersecurity

- **Strengthening AI data center security to mitigate cyber threats and protect AI workloads.** AI data centers house massive computational resources, making them prime cyberattack targets. Advanced security measures are necessary to prevent unauthorized access and data breaches. Adopt Zero Trust security architecture for AI data centers, enforcing *CISA's Zero Trust Maturity Model* to restrict lateral movement and insider threats (CISA, 2023). Secure AI model data against emerging cryptographic threats by requiring AI-specific encryption protocols aligned with *NIST's Post-Quantum Cryptography Standards* (NIST, 2024). Implement continuous threat monitoring in AI data centers, using *MITRE's ATT&CK Framework* to detect AI-specific cyber intrusions

(MITRE, 2024). Expand AI workload segmentation to prevent unauthorized data access, leveraging *NCSC (2024a).*

Cybersecurity

- **Strengthen AI model security against adversarial threats and cyberattacks.** AI systems are vulnerable to adversarial manipulation, requiring robust security frameworks to prevent malicious exploitation. Integrate AI adversarial resilience testing, using *MITRE ATLAS* to simulate attacks and enhance AI model robustness (MITRE, 2024). Develop AI-specific access control frameworks, following *NIST's AI Risk Management Framework* to prevent unauthorized model manipulation (NIST, 2023). AI security certifications are required, and compliance with *ISO/IEC 42001 AI Management Systems* is enforced to ensure that AI models meet cybersecurity best practices (ISO, 2024).

Deployment Security and AI Model Attack Prevention

- **Ensure AI security throughout the deployment pipeline.** AI models deployed in cloud, edge, and on-premises environments must be hardened against cyber threats. Establish AI model provenance tracking using *NIST's AI Bias and Security Testing Framework* to detect tampered models (NIST, 2024). Enforce AI API security best practices, applying *OWASP AI Security Guidelines* to mitigate injection attacks on AI-powered services (OWASP, 2024). Expand AI attack response mechanisms, integrating *CISA's Cyber Incident Response Playbooks* for AI-driven systems (CISA, 2024).

Technical and Safety Standards

- **Develop AI safety and cybersecurity standards to ensure trustworthiness.** AI systems must meet rigorous technical and ethical standards to ensure security and compliance. Align AI safety regulations with international frameworks, following *OECD AI Security Guidelines* for interoperability (OECD, 2024). Expand AI bias and fairness testing, leveraging *IEEE's AI Ethics Standards* to reduce discriminatory AI outcomes (IEEE, 2024). Require AI cybersecurity audits, enforcing compliance with *FISMA and NIST SP 800-53* for AI deployments in government systems (OMB, 2024).

National Security and Defense

- **Enhance AI applications for cybersecurity, intelligence, and military operations.** AI is a critical enabler of national defense and must be secured against adversarial threats. Deploy AI-driven cyber defense solutions, integrating *DOD's AI Cybersecurity Strategy* to protect U.S. military networks (DOD, 2023). Expand AI-enabled threat intelligence, leveraging *NSA's* (March, 2024 Report). Use Secure Cloud Key Management Practices. Mandate AI red-teaming in defense applications, requiring adversarial testing for autonomous defense systems (Brand, 2025).

Risk, Regulation, and Governance

- **The U.S. must establish comprehensive AI regulations and frameworks to ensure responsible development, deployment, and use while balancing innovation and risk mitigation.** The European Union's Artificial Intelligence Act is a notable example of this approach, showcasing a structured framework for regulating AI (Future of Life Institute, 2024). The regulations must address different types of AI systems, classifying each in terms of risk. Clear definitions of AI applications and legal responsibilities will prevent

ambiguity for developers, deployers, and users. The regulations must specify compliance obligations, enforcement mechanisms, and legal consequences for violations, ensuring accountability throughout AI development and use. AI regulations must consider strategic factors, including public impact, national security, and economic stability.

- **To effectively develop regulations and frameworks, entities such as the NIST should be consulted and utilized, building upon existing frameworks and expanding them to address emerging AI challenges.** NIST's AI Risk Management Framework (AI RMF) provides a structured approach to identifying, assessing, and mitigating AI risks, making it a strong foundation for national AI regulations (NIST, 2023). Policymakers should work with NIST and similar entities to refine and expand existing frameworks, incorporating AI-specific risk assessments tailored to public safety, national security, and economic stability.

- **International collaboration is crucial in establishing effective AI regulation and governance.** The U.S. can share research, gain insights, standardize AI guidelines, and foster ethical and safe AI development and usage by building international partnerships.

- **Ensure compliance with data regulation standards.** The U.S. must mandate AI developers to comply with data regulation standards such as the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016) and the California Consumer Privacy Act (CCPA) (California State Legislature, 2018).

Model Development

- **Transparency and accountability should be encouraged and enforced throughout the development of AI models.** Mandating AI developers to disclose information about their models' capabilities, limitations, and data sources enables external scrutiny for positive growth and fosters public trust in AI.

- **Establish standardized safety testing to ensure that AI development is safe before public use.** AI model safety evaluations should identify and mitigate potential security or ethical risks. Safety evaluations must ensure that the AI system operates as intended while not violating human or constitutional rights, such as censorship and freedom of speech.

Data Privacy and Security Throughout the AI Lifecycle

- **Leverage privacy-preserving AI techniques essential for secure data processing.** Organizations should integrate privacy-enhancing technologies (PETs) such as federated learning, differential privacy, and homomorphic encryption to mitigate risks associated with AI model training. These techniques allow AI models to process sensitive data without exposing raw data to external entities. PETs help maintain user privacy while enabling AI advancement (NIST, 2024).

References

Allen, Gregory C. 7 March 2025. *DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race*. Center for Strategic and International Studies. https://www.csis.org/analysis/deepseek-huawei-export-controls-and-future-us-china-ai-race

Brand, A. 14 February 2025. *DARPA seeks to develop "ai red team" to stress test AI Systems*. Journal of Electromagnetic Dominance. https://www.jedonline.com/2025/02/14/darpa-seeks-to-develop-ai-red-team-to-stress-test-ai-systems/

Bureau of Industry and Security. 13 January 2025. *Biden-Harris Administration Announces Regulatory Framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology*. https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion

Burner, Darcy. 13 May 2023. *Five Ways to Revitalize American Manufacturing*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2023/03/13/five-ways-to-revitalize-american-manufacturing/

Brynjolfsson, E., & McAfee, A. 2023. *The AI Revolution and Market Competition*. Harvard Business Review.

California State Legislature. 2018. *California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798. 100 et seq*. https://oag.ca.gov/privacy/ccpa

CISA. April 2023. *Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/zero-trust-maturity-model

CISA. 2024. *Secure Cloud Business Applications.* Technical reference architecture (TRA): CISA. https://www.cisa.gov/resources-tools/services/technical-reference-architecture-tra

Council on Foreign Relations. 17 September 2024. *Territorial Disputes in the South China Sea*. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

DOD. November 2023. *Data, analytics, and Artificial Intelligence Adoption Strategy*. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

European Commission. 2024. *AI Regulation and Antitrust Measures in the Digital Economy*. European Union Reports.

European Parliament and Council of the European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union. L 119, 1-88. https://gdpr-info.eu/

Feldman, B., Martin, E., & Skop, J. 2024. *Decentralized AI and the Future of Cloud Computing*. Journal of Emerging Technologies.

Future of Life Institute. 27 February 2024. *High-level summary of the AI Act. EU Artificial Intelligence Act.* https://artificialintelligenceact.eu/high-level-summary/

Godefroy, J. 7 March 2024. *How does artificial intelligence affect intellectual property protection?* Rouse. https://rouse.com/insights/news/2024/how-does-artificial-intelligence-affect-intellectual-property-protection

Helmus, Todd C., Romita-Grocholski, Krista, Liggett, Tyler, Rhoades, Ashley L., Savitz, Scott, and Palmer, Keytin. 20 November 2024. *Understanding and Countering China's Maritime Gray Zone Operations*. https://www.rand.org/pubs/research_reports/RRA2954-1.html

IEEE. January 2025. IEEE Standard for Algorithmic Bias Considerations 7003-2024. https://ieeexplore.ieee.org/servlet/opac?punumber=10851953

Intel. November 2024. *Intel Ohio: The Silicon Heartland*. https://download.intel.com/newsroom/2024/corporate/Intel-Ohio-The-Silicon-Heartland.pdf

Investopedia. 6 June 2024. *Public-Private Partnerships (PPPs): Definition, How They Work, and Examples*. https://www.investopedia.com/terms/p/public-private-partnerships.asp

ISO/IEC 27001:2022 – Information Security Management. ISO. 25 October 2022. https://www.iso.org/standard/27001

ISO. 18 December 2023. *Information technology — Artificial intelligence — Management system*. ISO/IEC 42001:2023. https://www.iso.org/standard/81230.html

Korinek, A., & Vipra, J. 27 March 2024. *AI Monopolies*. Economic Policy. https://www.economic-policy.org/79th-economic-policy-panel/ai-monopolies/

Korinek, A., & Vipra, A. 2025. *The Cost of AI Development and Its Economic Impact*. Epoch Research Institute.

Mitchell, M. 2023. *Artificial Intelligence: A Guide for Thinking Humans*. Princeton University Press.

MITRE. 2025. *Mitre Atlas*. MITRE ATLAS. https://atlas.mitre.org/

National Conference of State Legislatures. 16 February 2017. *Building Up: How States Utilize Public-Private Partnerships for Social and Vertical Infrastructure*. https://www.ncsl.org/transportation/building-up-how-states-utilize-public-private-partnerships-for-social-vertical-infrastructure

National Institute of Standards and Technology. 2023. *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

National Institute of Standards and Technology. 2024. *Artificial intelligence risk management framework (NIST AI 600-1)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

NIST. 31 January 2025. *NIST AI 600-1 Ai Risk Management Framework*. NIST AI 600-1. https://www.nist.gov/itl/ai-risk-management-framework

NIST. 4 May 2018. *Platform Firmware Resiliency Guidelines*. https://csrc.nist.gov/pubs/sp/800/193/final

NIST. February 2022. *Secure software development framework (SSDF) version 1.1*. NIST Special Publication 800-218. https://doi.org/10.6028/NIST.SP.800-218

NIST. November 2024. *Transition to Post-Quantum Cryptography Standards*. NIST IR 8547. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

NCSC. April 2024. *Deploying AI Systems Securely*. Joint Cybersecurity Information. https://media.defense.gov/2024/apr/15/2003439257/-1/-1/0/csi-deploying-ai-systems-securely.pdf

NCUA. 1 November 2024. *NCUA Artificial Intelligence Compliance plan*. https://ncua.gov/ai/ncua-artificial-intelligence-compliance-plan

NSA. March 2024. Use Secure Cloud Key Management Practices. https://media.defense.gov/2024/Mar/07/2003407858/-1/-1/0/CSI-CloudTop10-Key-Management.PDF

NCSC. (2024a). Guidelines for secure AI System Development. https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF

OECD. AI Policy Observatory. 2024. *AI Market Regulation and Fair Competition Strategies*. OECD Publications.

OECD. June 2024. *AI, Data Governance, and Privacy*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf

OBM. October 2024. *Fact sheet: OMB issues guidance to advance the responsible acquisition of AI in government | OMB | The White House*. National Archives and Records Administration. https://bidenwhitehouse.archives.gov/omb/briefing-room/2024/10/03/fact-sheet-omb-issues-guidance-to-advance-the-responsible-acquisition-of-ai-in-government/

OWASP. 2024. AI Security and Privacy Guide. https://owasp.org/www-project-ai-security-and-privacy-guide/

Office of the Federal Register. January 2025. Removing Barriers to American Leadership in Artificial Intelligence. Executive Order 14179. https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

Plotinsky D. 9 April 2024. *Existing and Proposed Federal AI Regulation in the United States*. Morgan Lewis. https://www.morganlewis.com/pubs/2024/04/existing-and-proposed-federal-ai-regulation-in-the-united-states

Rojas, Olivia. 26 November 2024. *The Tax Impact of the CHIPS Act on Semiconductor Manufacturing*. NC State University – Poole Thought Leadership. Retrieved https://poole.ncsu.edu/thought-leadership/article/the-tax-impact-of-the-chips-act-on-semiconductor-manufacturing/

Semiconductor Industry Association. September 2020. *Turning the Tide for Semiconductor Manufacturing in the U.S*. https://www.semiconductors.org/turning-the-tide-for-semiconductor-manufacturing-in-the-u-s/

Silicon Heartland. December 2024. *Silicon Heartland*. City of New Albany (OH). https://siliconheartland.newalbanyohio.org/

Smith, Spencer. 10 December 2024. *Will Memphis Pay a Price for Elon Musk's xAI "Colossus" Bait and Switch?* Southern Alliance for Clean Energy. https://www.cleanenergy.org/blog/will-memphis-pay-a-price-for-elon-musks-xai-colossus-bait-switch/

Spencer, Thomas and Singh, Siddharth. 18 October 2024. *What the Data Centre and AI Boom Could Mean for the Energy Sector*. International Energy Agency. https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector

Stackpole, Beth. 7 January 2025. *AI Has High Data Center Energy Costs – But There Are Solutions*. MIT Sloan School of Management. https://mitsloan.mit.edu/ideas-made-to-matter/ai-has-high-data-center-energy-costs-there-are-solutions

Suwanmatajarn, P. 10 March 2024. *Will AI bring the death to IP enforcement work*. Lexology. https://www.lexology.com/library/detail.aspx?g=2fff9b2a-cb52-41cf-bc70-8698f62ae919

Thadani, Akhil and Allen, Gregory C. *Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Region*. Center for Strategic and International Studies. https://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region

Trotolo, F., Hayat, H., & Hayat, D. 26 February 2025. *The cost of implementing AI in a business: A comprehensive analysis*. Walturn. https://www.walturn.com/insights/the-cost-of-implementing-ai-in-a-business-a-comprehensive-analysis

Weinstein, E. S., & Wolf, K. 5 July 2023. *For Export Controls on AI, Don't Forget the "Catch-All" Basics*. Center for Security and Emerging Technology. https://cset.georgetown.edu/article/dont-forget-the-catch-all-basics-ai-export-controls/

Zhai, Guankai. 28 August 2024. *Bringing Manufacturing Back to the U.S.: Easier Said Than Done*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2024/08/28/bringing-manufacturing-back-to-the-us-easier-said-than-done/