Executive Order 14110: Safe, Secure, and Trustworthy Artificial Intelligence

November 6th, 2023

Summary

President Biden's new executive order on artificial intelligence introduces some of the first mandatory requirements for both contractors and government regarding AI. President Biden released the executive order on October 30th, 2023. Despite the introduction of of these requirements, many of the directives within the order continue to build frameworks, principles, and guidelines around AI, rather than taking direct regulatory action. The order also encourages Federal agencies to use their own regulatory power as they deem appropriate. President Biden has called on Congress to bolster the new executive order with comprehensive AI legislation.

For more information on Carahsoft's AI portfolio, please visit our website or call (571) 591-6040.

Leveraging the Executive Order for Business

The White House has released an implementation guide for the Executive Order highlighting different areas that agencies should prioritize removing barriers to AI adoption.

IT Infrastructure

Agencies should ensure that their AI projects have access to adequate IT infrastructure, including high-performance computing infrastructure specialized for AI training and inference, where necessary. The implementation guide encourages agencies to ensure their equipment is AI-ready. To meet this goal, many agencies will likely need to acquire or modernize their existing systems.

Data

Agencies should develop adequate infrastructure and capacity to sufficiently curate agency datasets for use in training, testing, and operating AI. Agencies should also explore the utility of public access datasets and encourage their use, where appropriate and consistent with the data practices outlined in this memorandum, to help develop, test, and maintain AI applications. There are opportunities here to assist agencies in data labelling and data management to ensure AI readiness.

Cybersecurity

Agencies should update, as necessary, cybersecurity authorization processes to better address the needs of AI applications, including to advance the use of continuous authorizations for AI. Agency authorizing officials should also prioritize generative AI and other critical emerging technologies in Authorizations to Operate (ATO) and any other applicable release or oversight processes. Agencies will begin integrated generative AI into their ATO process and will likely need contractor support for this. Likewise, a new influx of ATOs around AI will require enhanced cybersecurity capabilities for agencies.

Workforce

Agencies should take full advantage of available special hiring and retention authorities to fill gaps in AI talent, encouraging applications from individuals with diverse perspectives and experiences, and ensure the use of recruitment best practices for AI positions, such as descriptive job titles and skills-based assessments. The government needs help training its employees to be AI-ready as well as building out the workforce itself.

Generative AI

In addition to heeding the guidance provided in Section 10.1(f) of the AI Executive Order, agencies should assess potential beneficial use cases of generative AI in their missions and establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk. New opportunities around generative AI are likely to arise in the coming months as agencies establish more clear policies around its use.

Major Provisions

- **Mandatory Red Team Reporting for Contractors:** AI developers who produce algorithms that may pose a risk to "national security, national economic security, or national public health and safety" will be required in accordance with the Defense Production Act to report when models are being trained and any results from every red-team test. Contractors who meet certain requirements will be required to provide these safety testing results to the government.
- **Chief Artificial Intelligence Officers:** Within 60 days of issuance, agencies must establish a Chief Artificial Intelligence Officer. These new positions will help centralize AI efforts and provide clearer leadership within agencies.
- **Prioritizing TMF Funding for AI:** The Technology Modernization Fund (TMF) will consider prioritizing AI and generative AI projects for their funding over the next year. This will open up considerably more funding for federal AI modernization projects.

Agency Actions in the Executive Order

Department of Commerce (DOC)

Federal AI Watermarking: The DOC will develop guidance for content authentication and watermarking for AI-generated content. These tools will be used by Federal agencies to mark their content ensuring authenticity.

Department of Education (DoED)

AI in Education: The Federal government will create resources to help educators deploy AI-enabled tools for teaching.

Department of Energy (DOE)

Apply New Red Teaming Stands: DOE build out AI testbeds and assist with efforts to monitor AI-enabled chemical, biological, radiological, nuclear, and cybersecurity risks.

Department of Health & Human Services (HHS)

AI-Enabled Bioengineering Standards: Agencies involved in life-science projects must establish standards regarding AI in biological synthesis screening to protect against AI-enabled, dangerous bioengineering. These standards will be a requirement to receive continued funding.

Ethical Use of AI in Healthcare: Addressing the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services administered by the Secretary, such as to promote: assessment of access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers; and analysis of whether algorithmic systems in use by benefit programs achieve equitable and just outcomes.

Healthcare Safety Program: HHS will establish a program to receive reports and address instances of unsafe healthcare practices involving AI.

Department of Homeland Security (DHS)

Incentivizing AI Workforce: DHS will make amendments ot the visa process to incentivize individuals with artificial intelligence experience to work in the United States.

Apply New Red Teaming Stands: The Department of Homeland Security will apply NIST red teaming standards to critical infrastructure sectors and establish the AI Safety and Security Board. They will also work alongside DOE to address AI systems' threats to critical infrastructure, as well as chemical, biological, radiological, nuclear, and cybersecurity risks. Together, these are the most significant actions ever taken by any government to advance the field of AI safety.

Department of Justice (DOJ)

AI in Criminal Justice: The DOJ and Federal civil rights offices will develop guidelines for investigating and prosecuting cases related to AI discrimination. Best practices on use of AI in sentencing, parole and probation, pretrial release and detention, risk assessments, surveillance, crime forecasting and predictive policing, and forensic analysis will also be developed.

Department of Labor (DOL)

Worker Protection: DOL will develop best practices for employers to mitigate AI's potential harm to employees.

National Institute of Standards and Technology (NIST)

Standards Development: Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy. The National Institute of Standards and Technology will set the rigorous standards for extensive red-team testing to ensure safety before public release.

Office of Personnel Management (OPM)

Hiring Guidance: OPM will develop guidance on the use of generative AI for work by the Federal workforce. They are also launching a new jobs portal through the White House's AI.gov website.

Other Provisions

Cybersecurity: An advanced cybersecurity program will be established to find and fix vulnerabilities in algorithms and will expand upon the existing AI Cyber Challenge. DHS will develop a pilot project to deploy AI and LLMs for cybersecurity to discover and remediate vulnerabilities in government systems.

Expanding AI Competition in the Marketplace: The National Semiconductor Technology Center will open up funding to startups and small businesses.

Discrimination Prevention: The Federal government will establish new guidelines for landlords, Federal benefits programs, and Federal contractors on AI use and discrimination.

National Security Guidance: A new national security memorandum will be produced that outlines safe, ethical, and effective use of AI within the military.

Training Data Privacy: The Federal government will support the creation of techniques that help ensure the privacy of data used to train AI. NSF will help promote this and funding will go to a Research Coordination Network to help develop privacy-enhancing tools.

Commercial Data Evaluation: The Federal government will evaluate how it collects and uses commercially available, specifically data acquired from data brokers. The government will focus heavily on data containing personally identifiable information.

IP Theft Guidance: The US Copyright Office and Attorney General will develop guidance to mitigate and evaluate AI-based IP

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®, supporting Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services and training through hundreds of contract vehicles.

About Carahsoft AI

Carahsoft's technology portfolio includes the best-of-breed AI, ML and HPC capabilities to help government agencies connect technology and industry partners with solutions that fulfill mission needs. Our solution and service providers help agencies harness information and insights to improve mission-critical decisions.

About Carahsoft Market Research

The Market Research team supplies value to our vendor partner ecosystem by providing actionable government intelligence. Our team helps market to the intent & need of the customer, build a strategic audience & campaign, provide content on government trends, create creative lead Generation from trends, legislation, and news, and provide strategic account planning and tailored territory & technology reports.

Additional Resources

- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence
- Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence
- DoD: Data, Analytics, and Artificial Intelligence Adoption Strategy
- Industry Letter on President Biden's Executive Order