BIDEN EXECUTIVE ORDER ON AI: WHAT BUSINESSES CAN DO (FOR NOW) ABOUT THE SAFETY AND SECURITY MANDATES

On November 16, 2023, we published a blog titled "What businesses need to know (for now) about the Biden Executive Order on AI", where we summarized President Joe Biden's Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence (***EO***) in a global context and offered practical recommendations for business use. This blog focuses on the safety and security aspects of the EO and similarly, seeks to offer practical guidance and perspective.

Ensuring the Safety and Security of AI Technology: Overview

Although the EO is broadly framed across eight general areas, the Section titled "Ensuring the Safety and Security of AI Technology" contains the EO's arguably most specific and technical requirements. While the Section mandates the Secretary of Commerce, the Secretary of the Treasury, the Secretary of Homeland Security, and other agencies to take actions with direct impact on the Federal Government, it also imposes requirements on and impacts specific businesses:

- Companies developing or "demonstrating an intent to develop" potential dual-use foundation models[1] (***Dual-Use Foundation Model Developers***)
- Organizations and individuals that acquire, develop, or possess a potential large-scale computing cluster[2] (***Large-Scale Computing Clusters Developers***)
- United States Infrastructure as a Service Providers[3] and foreign resellers of their products
- Critical infrastructure owners and operators
- Financial institutions
- Providers of synthetic nucleic acid sequences[4], agencies that fund life sciences research and other life sciences stakeholders
- Businesses across all industries

Ensuring the Safety and Security of AI Technology: Deep-Dive

Below we summarize key requirements and recommended next steps for specific businesses.

Dual-Use Foundation Model Developers and Large-Scale Computing Clusters Developers

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
The Secretary of Commerce will require Dual-Use Foundation Model Developers to provide the Federal Government with information, reports or records regarding ongoing or planned activities for training, developing, or producing dual-use foundation models; ownership and possession of model weights and related physical and cybersecurity measures; the results of any AI red-team testing; and related measures based on National Institute of Standards and Technology (***NIST***) standards. The EO specifically calls out results relating to biological weapons acquisition and use by non-state actors, discovery of software vulnerabilities, and use of software to influence real or virtual events. The EO also requires Large-Scale Computing Clusters Developers to report their activities to the Federal Government, including the existence, location and required computing power for each cluster.	By January 28, 2024 (within 90 days of the EO)	Assess whether your business uses or plans to use dual-foundation models or large-scale computing clusters. If yes: (i) obtain detailed understanding of what they are, how they work, and how you will use them; and (ii) consider whether and how you will be able to comply with the specific evolving requirements of the EO, including by assessing any relevant arrangements with third parties. This analysis should also consider the EO's other focus areas, including relating to IP and privacy.

US Infrastructure as a Service Providers and Foreign Resellers of Their Products

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
The Secretary of Commerce will propose regulations that require US Infrastructure as a Service Providers (***US IaaS Providers***) to submit reports to the Secretary when a foreign person transacts with such provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a ***training run***). Such regulations will prohibit any foreign reseller of US IaaS Products from doing so, unless it submits a report, which the US IaaS Provider will submit to the Secretary of Commerce, detailing instances of training runs. The Secretary of Commerce will also propose regulations that, among other provisions, require US IaaS Providers to ensure that foreign resellers of their products verify the identity of any foreign person that obtains an IaaS account from such reseller. The EO contains minimum detailed requirements for such regulations, including rules for documentation and procedures, and record keeping.	By January 28, 2024 (within 90 days of the EO)	Consider: (i) if you fall within the definition of "**United States Infrastructure as a Service Provider**". If yes, or potentially yes, review your existing processes and frameworks to ensure that you can produce reports identified in this Section; (ii) your relationships with foreign resellers and such resellers' ability to provide required reporting and to otherwise comply with the requirements; and (iii) how these developments tie to your existing contractual commitments and parameters and whether you need new relationships. If you are a foreign reseller of US IaaS products, review your ability to comply with these requirements.

Critical Infrastructure Owners and Operators

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
Heads of relevant agencies will assess potential risks and mitigants related to the use of AI in critical infrastructure sectors, including ways in which AI may make critical infrastructure systems vulnerable to critical failures, physical attacks, and cyber-attacks.	By January 28, 2024 (within 90 days of the EO)	Revisit your existing AI cybersecurity risks and existing processes and systems to address any known vulnerabilities and opportunities. Study the AI Risk Management Framework, NIST AI 100-1 and related resources to assess how your organization meets these requirements today. Although the NIST Framework is voluntary today, it will play a pivotal role in the implementation of the EO. Consider opportunities to engage with NIST and keep an eye out for upcoming developments in this space. If you are a government contractor, these actions are particularly important in view of the anticipated pilot projects.
The Secretary of Homeland Security will incorporate the AI Risk Management Framework, NIST AI 100-1 and other applicable security guidance into safety and security guidelines for critical infrastructure owners and operators. Within 240 days of completion of such guidelines, relevant heads will coordinate the guidelines' implementation. The Secretary of Defense and the Secretary of Homeland Security will each complete an operational pilot project to test AI capabilities to aid in the discovery and remediation of vulnerabilities in critical US Government software, systems and networks, to be followed, within 270 days of the EO, by reports on the results of actions taken pursuant to these pilots, including description of vulnerabilities found and fixed and lessons learned for use of AI for cyber defense.	By April 27, 2024 (within 180 days of the EO) and the specific follow-on dates noted in the "Relevant Requirements" column	

Financial Institutions

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
The Secretary of the Treasury will issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.	By March 28, 2024 (within 150 days of the EO)	Revisit your existing AI cybersecurity risks and existing processes and systems to address any known vulnerabilities and opportunities. Study the AI Risk Management Framework, NIST AI 100-1 and related resources to assess how your organization meets these requirements today. Although the NIST Framework is voluntary today, it will play a pivotal role in the implementation of the EO. Consider opportunities to engage with NIST and keep an eye out for upcoming developments in this space.

Providers of Synthetic Nucleic Acid Sequences, Agencies that Fund Life Sciences Research and Other Life Sciences Stakeholders

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
Various government officials will establish a framework to encourage providers of synthetic nucleic acid sequences to implement comprehensive screening mechanisms. The Secretary of Commerce will engage with the industry and relevant stakeholders, informed by the above framework, to develop and refine for use by synthetic nucleic acid sequence providers specifications, best practices, and technical implementation guides.	By April 27, 2024 (within 180 days of the EO)	Review your existing systems and processes as well as contractual commitments for potential changes to ensure compliance with this focus area. Consider opportunities to engage with NIST and keep an eye out for upcoming developments in this space.
Agencies that fund life-sciences research will ensure that synthetic nucleic acid procurement is conducted through providers or manufacturers that adhere to the framework. Such compliance will also be reviewed by various regulators.	By October 24, 2024 (within 180 days of the establishment of the above framework)	

Businesses Across Industries

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
The Secretary of Commerce, acting through the Director of NIST, in coordination with the heads of other relevant agencies will: • Establish guidelines and best practices to deploy safe, secure, and trustworthy AI systems including by developing companion resources to the: (i) AI Risk Management Framework, NIST AI 100-1, for generative AI; and (ii) Secure Software Development Framework for generative AI and for dual-use foundation models. • Establish guidelines to enable AI developers to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems.	By July 26, 2024 (within 270 days of the EO)	Study the AI Risk Management Framework, NIST AI 100-1 and related resources to assess how your organization meets these requirements today. Although the NIST Framework is voluntary today, it will play a pivotal role in the implementation of the EO. Consider opportunities to engage with NIST and keep an eye out for upcoming developments in this space. Study the Secure Software Development Framework and assess how your organization meets these requirements today. Cohesively understand what AI red-teaming tests your organization performs today, consider improvements, and monitor ongoing developments.

Relevant Requirements	Timeline	What Your Business Can Do (For Now)
The EO's sub-section titled "Reducing the Risks Posed by Synthetic Content" focuses on a need to establish authenticity and provenance of synthetic and non-synthetic digital content produced by the Federal Government or on its behalf. The Secretary of Commerce, in consultation with other relevant agencies and heads, will submit a report identifying existing standards and practices and the potential development of new standards and tools for e.g., authenticating content and tracking its provenance, labelling of synthetic content by e.g., watermarking, and detecting synthetic content.	By June 26, 2024 (within 240 days of the EO)	Although these provisions are focused on Federal Government's use of these tools, there is ongoing attention to this area in the B2B and B2C context. For example, Congress has introduced the AI Labelling Act that requires clear and conspicuous disclosure of AI generated content across all media types. There is room for discussion and debate around practical implications and usefulness of such labelling as e.g., it is not adequate for works produced through collaboration between AI and humans.
The Secretary of Commerce will develop guidance regarding tools and practices for digital content authentication and detection measures.	By December 23, 2024 (within 180 days of the report)	
Various regulators will issue guidance to agencies for labelling and authenticating official US Government digital content.	By June 21, 2025 (within 180 days after the Secretary of Commerce's guidance)	

Opportunities to Engage in Rulemaking

In addition to outlining specific requirements noted above, the EO also offers opportunities for businesses to engage in rulemaking. It tasks various agencies to seek input from experts in developing and implementing AI related capabilities as follows:

Opportunity	Timeline	Relevant Stakeholders	What Your Business Can Do (For Now)
The Secretary of Energy, in coordination with the heads of other agencies, will develop and implement a plan for developing the Department of Energy's AI model evaluation tools and AI testbeds. At a minimum, the Secretary will develop tools to evaluate AI capabilities to generate outputs that may represent nuclear, non-proliferation, biological, chemical, critical infrastructure and energy-security threats or hazards.	By July 26, 2024 (within 270 days of the EO)	The Secretary will consult with private AI laboratories, academia, civil society, and third-party evaluators.	Consider contacting the Secretary of Energy to weigh in on and participate in this plan.
The Secretary of Homeland Security will establish an AI Safety and Security Board as an advisory committee relating to AI usage in critical infrastructure.	No date specified	The advisory committee will consist of experts from the private sector, academia, and government.	Consider contacting the Secretary of Homeland Security to serve on this committee.

Opportunity	Timeline	Relevant Stakeholders	What Your Business Can Do (For Now)
The Secretary of Homeland Security will evaluate AI model capabilities to present threats and submit a report to the President.	By April 27, 2024 (within 180 days of the EO)	The Secretary of Homeland Security will consult with experts in AI and chemical, biological, radiological, or nuclear issues.	Consider contacting the Secretary of Homeland Security to assist with this report.
The Secretary of Commerce will evaluate considerations relating to dual-use foundation models for which the model weights are widely available.	By July 26, 2024 (within 270 days of the EO)	The Secretary will solicit input from the private sector, academia, civil society, and other stakeholders through public consultation process.	Consider contacting the Secretary of Commerce to weigh in on these considerations.

As we wrote in our first blog, we believe that the EO represents a meaningful step in the regulation of AI technologies as it aims to advance a comprehensive framework for the safe, secure, and trustworthy use of AI. The EO is complimented by other ongoing Federal Government initiatives, including, most recently, the National Defense Authorization Act for Fiscal Year 2024, which contains provisions relating to a bug bounty program for the Pentagon to detect flaws in foundational AI models used by the military, a prize for detecting and watermarking AI-generated content, and the establishment of a Chief Digital and Artificial Intelligence Officer Governing Council responsible for AI deployment for the Pentagon. Businesses are well advised to actively monitor the EO and related updates and developments and to take proactive steps to understand and comply with the evolving requirements.

Clifford Chance and Artificial Intelligence

Clifford Chance is following AI developments very closely and will be conducting subsequent seminars and publishing additional articles on new AI laws and regulations. If you are interested in receiving information from Clifford Chance on these topics, please reach out to your usual Clifford chance contact or complete this preferences form.

Clifford Chance was the only law firm that participated as a partner in the recent AI Fringe, which brought together civil society, academic, commercial, advocacy and government stakeholders in London in October 2023 – all the sessions can be found here.

Clifford Chance has also recently published an insightful report on "Responsible AI in Practice", which examines public attitudes to many of the issues discussed in this article.

Endnotes

1 The term "**dual-use foundation model**" means "an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by: (i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons; (ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber-attacks; or (iii) permitting the evasion of human control or oversight through means of deception or obfuscation. Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities".

   While this definition is expected to be refined, the following are in scope of the reporting requirements of the EO: "any model that was trained using a quantity of computing power greater than 10 to 26th power integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10 to 23rd power integer or floating-point operations."

2 The term "**large scale computing clusters**" is not defined. Until further developments, the following are in scope of the reporting requirements: "any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10 to 20th power integer or floating-point operations per second for training AI."

3 The term "**United States Infrastructure as a Service Provider**" means any United States individual or entity "that offers any Infrastructure as a Service Product" and "**Infrastructure as a Service Product**" means "any product or service offered to a consumer, including complimentary or 'trial' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications. The consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. The term is inclusive of 'managed' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and 'unmanaged' products or services, in which the provider is only responsible for ensuring that the product is available to the consumer. The term is also inclusive of 'virtualized' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (e.g., 'virtual private servers'), and 'dedicated' products or services in which the total computing resources of a physical machine are provided to a single person (e.g., 'bare-metal' servers)."

4 The term "**synthetic nucleic acid sequences**" is not defined but "**synthetic nucleic acids**" are "a type of biomolecule redesigned through synthetic-biology methods". The term "**synthetic biology**" means "a field of science that involves redesigning organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics".

AUTHORS

Inna Jackson
Tech Knowledge & Innovation Attorney
New York
T: +1 212 878 3292
E: inna.jackson@cliffordchance.com

James McPhillips
Partner
Washington DC
T: +1 202 912 5010
E: james.mcphillips@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2312-009077