CORVINUS LAW PAPERS

ISSN 2416-0415

1/2024

Theodore S. Boone

An Examination Of Certain Key Features Of The New White House Executive Order On Artificial Intelligence

CORVINUS UNIVERSITY OF BUDAPEST

Corvinus Law Papers

CLP 1/2024

The primary purpose of the Corvinus Law Papers (CLP) is to publish the results of research projects performed by those connected to the Department of Business Law as research reports, working papers, essays and academic papers. The CLP also publishes supplementary texts to be used for practical and theoretical training of students.

Address of the Editorial Board:

Corvinus Law Papers
1093 Budapest, Fővám tér 8. III. emelet 321/A

Publisher:

Corvinus University of Budapest
H-1093 Budapest, Fővám tér 8.

Responsible for the edition:

Dániel Bán

ISSN 2416-0415

AN EXAMINATION OF CERTAIN KEY FEATURES OF THE NEW WHITE HOUSE EXECUTIVE ORDER ON ARTIFICIAL INTELLIGENCE

By

Theodore S. Boone[1]

theodore.boone@uni-corvinus.hu

ABSTRACT

This article examines certain key features of the White House Executive Order on Artificial Intelligence issued on October 30, 2023. It places this Executive Order in the context of prior US governmental actions related to AI and discusses the legal strength of the Executive Order. The article takes the position that as much of the Executive Order consists of instructions to government agencies to develop guidance and draft regulations for further consideration the true impact of much of the Executive Order is yet to be seen. The article states that the most immediate direct impact on the private sector will be the Executive Order's private sector reporting requirements related to the development of dual-use foundation models and large scale computing clusters which pose risks to national security. The article states that the US National Institute of Standards and Technology will likely continue to play a central role in the evolution of AI regulatory initiatives and may continue to look to international AI related ISO and IEC standards when doing so, that red-teaming precedents from cybersecurity practices will likely be used to vet AI systems and that Know Your Customer requirements drawn from the example of the financial services sector may well be put in place for US based cloud service providers. The article states that given the content of the Executive Order and the inherent weaknesses in Executive Orders more generally it is unlikely that the US Congress' focus on potential AI legislation will cease.

KEY WORDS

Artificial Intelligence; AI; Executive Order; Risk Management; ISO; IEC; ISO/IEC, Cybersecurity; Red-Teaming; Dual Use Foundation Models; National Security; Know Your Customer; KYC; EU AI Act

1. INTRODUCTION

On October 30, 2023, a mere three days before leaders of governments and multilateral and non-governmental organizations, technology executives and academics convened at England's legendary Bletchley Park for the AI Safety Summit hosted by the UK, US President Joseph R.

[1] Member of the faculty of Corvinus University of Budapest and Of Counsel, Dentons Budapest.

Biden issued a new and wide-ranging Executive Order on Artificial Intelligence titled "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (the "White House AI Executive Order" or "Order").[2] The timing of the release of the White House AI Executive Order just before the Summit was hardly coincidental. Rather it was an effort to capture the international spotlight on the legal regulation of AI and present the United States as a leader and example in the field. The purpose of this article is to place the White House AI Executive Order within the context of prior US governmental activities related to the legal regulation of AI and to examine certain key features of the White House AI Executive Order.

2. US GOVERNMENET AI MILESTONES 1972 - 2020

The White House AI Executive Order is not the first or only significant action by the US government related to AI. From 1972 until its termination in 1995 the US Office of Technology Assessment provided US Congressional representatives with research and analysis on science and technology issues, including AI related issues. In 1991 the US government created the High Performance Computing and Communications Initiative designed to speed the development of high performance computers and their use both within the Federal government and in the economy more generally.[3] In 2016, the White House issued the National Artificial Intelligence Research and Development Strategic Plan.[4] The goal of the Plan was to set priorities for Federally funded AI research.

On February 11, 2019 US President Donald J. Trump issued an Executive Order titled "Maintaining American Leadership in Artificial Intelligence".[5] The Executive Order on Maintaining American Leadership in Artificial Intelligence provided that the policy of the US Government was to grow the scientific, technological, and economic leadership position of the United States in AI R&D and deployment through a coordinated Federal government strategy, termed the "American AI Initiative" and that this initiative was to be guided by five principles: (1) driving technological breakthroughs in AI; (2) fostering the development of appropriate technical standards; (3) providing training to individuals; (4) fostering public trust in AI technologies and protecting civil liberties, privacy, and US values in their application; and (5) promoting an international environment that supports US AI research and innovation and opens

[2] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024]. Artificial Intelligence is hereinafter sometimes referred to as "AI". The AI Safety Summit was held November 1-2, 2023 at Bletchley Park, Buckinghamshire, England. The stated aims of the Summit were to examine the risks of Artificial Intelligence and how such risks can be mitigated through international coordination. For further information on the Summit see https://www.gov.uk/government/topical-events/ai-safety-summit-2023 [Accessed January 14, 2024].

[3] See Committee on Physical, Mathematical, and Engineering Sciences; Federal Coordinating Council for Science, Engineering, and Technology; Office of Science and Technology Policy, Office of Science and Technology Policy. (1994) *High Performance Computing & Communications: Toward a National Information Infrastructure.* Washington, D.C., p. 1. In English. Available from: https://www.nitrd.gov/pubs/1994supplement/NITRD_Supplement-1994.pdf [Accessed January 16, 2024] and National Academies of Sciences, Engineering, and Medicine. (1994) *Interim Report on the Status of the High Performance Computing and Communications Initiative*. Washington, DC: The National Academies Press. In English. Available from: https://nap.nationalacademies.org/read/10525/chapter/1 [Accessed January 16, 2024].

[4] National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee. (2016) *The National Artificial Intelligence Research and Development Strategic Plan.* Washington, D.C. In English. Available from: https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf [Accessed January 16, 2024].

[5] *Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence.* (2019) United States. In English. Available from: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence [Accessed January 16, 2024].

markets for US AI industries while protecting critical AI technologies from acquisition by strategic competitors and adversarial nations.[6]

In 2020 the National Artificial Intelligence Initiative Act was enacted.[7] The National Artificial Intelligence Initiative Act established the ‘‘National Artificial Intelligence Initiative’’. The stated purpose of the Initiative was to, among other matters, ensure continued US leadership in AI research and development.[8] One of the requirements of the National Artificial Intelligence Initiative Act was to require the US Department of Commerce's National Institute of Standards and Technology (the "NIST") to advance standards for AI.[9] Methods specified under the National Artificial Intelligence Initiative Act pursuant to which the NIST could fulfil this requirement included supporting measurement research and development of best practices and voluntary standards for trustworthy artificial intelligence systems.[10] The National Artificial Intelligence Initiative Act also required the NIST to develop and periodically update, in collaboration with other public and private sector organizations, a voluntary risk management framework for trustworthy artificial intelligence systems.[11]

3. THE WHITE HOUSE AI BLUEPRINT FOR A BILL OF RIGHTS OF 2022

On October 4, 2022, the White House, via its Office of Science and Technology, issued the Blueprint for an AI Bill of Rights (the "White House AI Blueprint").[12] The White House AI Blueprint, which is the rough equivalent of a White Paper and is not legally binding, sought to provide a framework for the development of AI in a manner which protects the rights of US citizens. The use of the term "Bill of Rights" in the title of the White House AI Blueprint for an AI Bill of rights is the use of a term carrying the weight of US history behind it as the US Bill of Rights consists of the first ten Amendments to the US Constitution. These ten Amendments set out certain basic rights of US citizens in relation to their government. For example, these Amendments address freedom of speech, press and assembly and protection from unreasonable search and seizure.[13] The White House AI Blueprint was issued seven months after the European Union ("EU") issued a non-binding White Paper on AI.[14] Similar to the White House AI Blueprint, the EU AI White Paper sought to provide overarching guidance on the development of AI in a manner which protects EU citizens and EU fundamental rights. The White House AI Blueprint stated that in relation to AI the public should

---

[6] *Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence.* (2019) United States. In English. Available from: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence [Accessed January 16, 2024], Section 1.

[7] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024].

[8] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024], Section 5101 (a).

[9] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024], Section 5301.

[10] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024], Section 5301.

[11] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024], Section 5301.

[12] *Blueprint for an AI Bill of Rights.* (2022) United States. In English. Available from: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [Accessed January 16, 2024].

[13] *The US Bill of Rights, Constitution of the United States of America*. (1791) United States. In English. Available from: https://www.archives.gov/founding-docs/bill-of-rights-transcript [Accessed January 16, 2024].

[14] *European Commission White Paper On Artificial Intelligence – A European Approach to Excellence and Trust*. (2022) In English. Available from: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en [Accessed January 16, 2024].

be protected from (1) unsafe and ineffective systems; (2) discrimination by algorithms; (3) abusive data privacy practices; (4) the use of automated systems without notice and explanation; and (5) the use of automated systems without the ability to opt out or access of human to resolve who can address problems that arise. [15]

4. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY RISK MANAGEMENT FRAMEWORK OF 2023

In January 2023 the NIST issued an Artificial Intelligence Risk Management Framework (the "NIST AI Risk Management Framework").[16] As with the White House AI Blueprint, the NIST AI Risk Management Framework is not legally binding. However, unlike many of the other government initiatives related to AI which preceded it, the NIST AI Risk Management Framework moved well beyond general broad-brush statements of desired goals. Rather, the NIST AI Risk Management Framework set down practical guidance to assist both governmental entities and private sector actors on managing the risks associated with AI.

5. MAY 16, 2023 AI US SENATE HEARING OF MAY 16, 2023

On May 16, 2023 the U.S. Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law hosted a broad ranging hearing titled "Oversight of A.I.: Rules for Artificial Intelligence."[17] US Senators from both major US political parties participated hearing and three individuals testified before the Subcommittee: Samuel Altman, the CEO of OpenAI (the creator of ChatGPT); Christina Montgomery, the Chief Privacy & Trust Officer of IBM; and Gary Marcus, Professor Emeritus at New York University. The hearing focused on the potential for US Congressional legislative action relating to AI. During the course of the three-hour hearing several themes emerged. First, there appeared to be bi-partisan consensus among Senators and the parties testifying that the type of liability shield granted to internet services providers in 1996 under Section 230 of the 1996 Communications Decency Act should not be granted to providers of Generative AI systems such as ChatGPT.[18] Second, there appeared to be a consensus among the parties testifying that the proposed EU AI Act could serve as a model for US legislative action in that the EU AI Act, as currently proposed, would take a targeted risk based approach to AI related legislation.[19] As Montgomery stated in her testimony: " … the

[15] *Blueprint for an AI Bill of Rights.* (2022) United States. In English. Available from: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [Accessed January 16, 2024].

[16] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024].

[17] *Transcript of US Senate Judiciary Subcommittee Hearing on Oversight of AI* (2023) United States. Tech Policy.Press United States. In English Available from: https://www.techpolicy.press/transcript-senate-judiciary-subcommittee-hearing-on-oversight-of-ai/ [Accessed January 16, 2024].

[18] Section 230 of the 1996 Communications Decency Act states in part that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. 230 - Protection for private blocking and screening of offensive material (1996). United States. In English. Available from: 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu) [Accessed January 16, 2024].

[19] On April 21, 2021 the EU Commission issued a proposal for regulation by the EU of AI. See *European Commission Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence. Laying Down Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts* (2021) Available from: The Act | EU Artificial Intelligence Act [Accessed January16, 2024]; Since that time the EU Council and the EU Parliament have also issued drafts of the EU AI Act. On December 9, 2023 it was announced that the Eu Parliament and the EU Council had reached provisional agreement on a compromise text of the EU AI Act. See *Artificial Intelligence Act: deal on comprehensive rules for trustworthy*

conception of the EU AI Act is very consistent with this concept of precision regulation where you're regulating the use of the technology in context. So absolutely that approach makes a ton of sense…Different rules for different risks."[20] Third, the appeared to be a consensus among the parties testifying there is a need for Congress to step in to regulate AI. Marcus argued for safety reviews similar to those used by the US Food and Drug Administration and Altman floated the concept of an entirely new AI focused regulatory agency: "I would form a new agency that licenses any effort above a certain scale of capabilities and can take that license away and ensure compliance with safety standards."[21]

6. LEGAL EFFECT OF WHITE HOUSE EXECUTIVE ORDERS

When considering the possible impact of the White House AI Executive Order is it important to keep in mind that although Presidential Executive Orders such as the White House AI Executive Order are viewed as having the force of law they are by their nature generally considered to be a less powerful and stable form of US law than an Act of the US Congress. Executive Orders can be modified or nullified by the US Congress or a subsequent President. For example, in April 1992, President George H. W. Bush issued an Executive Order related to Federal contracting. President Bill Clinton revoked that Executive Order in February 1993. President George W. Bush revoked President Clinton's revocation of that Executive Order in February 2001. President Barak Obama then revoked President Bush's revocation of President Clinton's revocation of that Executive Order in January 2009.[22] Hence, the White House AI Executive Order, like all other Executive Orders, could be modified or nullified by the US Congress or a subsequent President.[23] It is also important to keep in mind that a US President cannot simply "declare law" through an Executive Order on a subject and of a scope of that President's choosing. Rather, the Presidential power to issue an Executive Order must be the result of a delegation of authority by the US Congress, based on the powers of the President under Article Two of the US Constitution or a combination of both. As a result of these limitations, Executive Orders may also be challenged in court on the basis of a President having exceeded the scope of Presidential authority.

7. CERTAIN KEY FEATURES OF THE WHITE HOUSE AI EXECUTIVE ORDER

7.1. PURPOSE

The White House AI Executive Order states that AI possesses "extraordinary potential for both promise and peril".[24] The Order states that the Biden Administration is placing the "highest

AI (2023), EU Parliament Press release. In English. Available from Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI | News | European Parliament (europa.eu)[Accessed January 16, 2024]. [19]

[20] *Transcript of US Senate Judiciary Subcommittee Hearing on Oversight of AI* (2023) United States. Tech Policy.Press In English Available from: https://www.techpolicy.press/transcript-senate-judiciary-subcommittee-hearing-on-oversight-of-ai/ [Accessed January 16, 2024].

[21] *Transcript of US Senate Judiciary Subcommittee Hearing on Oversight of AI* (2023) United States. Tech Policy.Press In English Available from: https://www.techpolicy.press/transcript-senate-judiciary-subcommittee-hearing-on-oversight-of-ai/ [Accessed January 16, 2024].

[22] *Presidential Transitions: Executive Orders* (2020) Congressional Research Service, United States. In English. p 2. Available from: Presidential Transitions: Executive Orders (fas.org) [Accessed January 16, 2024].

[23] For a detailed study of the manner in which US courts have considered Executive Orders see for example Newland E., (2015) *Executive Orders in Court*, The Yale Law Journal, Volume 124, Number 6, April 2015. Available from: https://www.yalelawjournal.org/note/executive-orders-in-court [Accessed January 16, 2024].

[24] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-

urgency" on the development of AI in a safe and responsible manner and it is for this reason that the White House is pushing forward a coordinated government wide effort on AI. [25]

7.2. SPECIFIC INSTRUCTIONS TO GOVERNMENT AGENCIES

The White House AI Executive Order contains a broad range of specific instructions to over 50 federal agencies and other entities to engage in more than 100 specific actions to implement the guidance set forth in the White House AI Executive Order, often including instructions to take specified actions by a stated deadline.[26] Key instructions in this regard include those instructions set forth below.

7.2.1 Developing Guidelines, Standards, and Best Practices for AI Safety and Security

(a) Instructions to Secretary of Commerce

(i) Guidelines to Promote Consensus Industry Standards

The White House AI Executive Order states that within 270 days of its issuance (that is, within 270 days of October 30, 2023) the Secretary of Commerce, acting through the Director of the NIST (the Government entity which as noted above issued the NIST AI Risk Management Framework), must establish guidelines to promote consensus industry standards for developing and deploying safe, secure, and trustworthy AI systems.[27]

Under the topic of developing consensus industry standards related to AI it is relevant to note that the NIST AI Risk Management Framework discussed above in several instances leveraged off of standards issued by the International Organization for Standardization (the "ISO") and International Electrotechnical Commission (the "IEC"), both international non-governmental organizations that that develop international standards.[28] Certain standards are issued jointly by the ISO and the IEC. For example the ISO and the IEC have issued a joint standard on AI concepts and terminology, known as ISO/IEC 22989:2022.[29] In the case of the NIST AI Risk Management Framework, the NIST AI Risk Management Framework leveraged off of and specifically referred to, ISO/IEC 22989:2022 when it set forth a definition of AI system.[30] The NIST AI Risk Management Framework also drew on standards issued by the ISO, the IEC or both organizations jointly for other definitions, such as definitions of "social

order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 1.

[25] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 1.

[26] *Highlights of the 2023 Executive Order on Artificial Intelligence for Congress* (2023) Congressional Research Service, United States. In English. p. 3. Available from: R47843 (congress.gov) [Accessed January 16, 2024].

[27] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.1.

[28] See ISO - About us and What IEC does (2024). In English. Available from: ISO - About us [Accessed January 16, 2024]. For a general discussion of the background, genesis and uses of ISO and IEC standards see *Using and referencing ISO and IEC standards to support public policy* (2024), ISO and IEC. In English. Available from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100358.pdf [Accessed January 16, 2024].

[29] *ISO/IEC 22989:2022, Information Technology Artificial intelligence concepts and terminology*, ISO. In English. Available from Publicly Available Standards (iso.org) [Accessed January 16, 2024].

[30] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024], p. 1.

responsibility", "sustainability" and "professional responsibility".[31] The NIST AI Risk Management Framework leveraged off of ISO Standards' definitions of "risk" and "risk management" to delineate types of harm which AI systems may cause, broken down into harm to people, harm to organizations and harm to an ecosystem.[32] The NIST AI Risk Management Framework based its discussion on definitions of "validation", "reliability", "accuracy", "robustness", "generalizability" established by the ISO and/or the ISO and the IEC. [33] In addition, when discussing the safety of AI systems the NIST AI Risk Management Framework noted "AI systems should "not under defined conditions, lead to a state in which human life, health, property, or the environment is endangered" (Source: is ISO/IEC TS 5723:2022)."[34] From these examples of the use of ISO and ISO/IEC standards by the NIST in the development of the NIST AI Risk Management Framework it is reasonable to presume that the NIST will continue to look to AI related standards and definitions created by the ISO and/or the ISO and the IEC, when working to fulfil the instructions to the Secretary of Commerce and the Director of the NIST to establish guidelines to promote consensus industry standards for developing and deploying safe, secure, and trustworthy AI systems.

(ii) Guidelines for Red-Team Testing

The White House AI Executive Order requires the Secretary of Commerce to within 270 days of its issuance establish guidelines for AI other than AI used in national security matters to guide developers of AI to conduct AI "red-teaming" tests to enable the deployment of safe, secure, and trustworthy AI systems.[35] The concept of the requirement to develop guidance for the use of such so-called "red-teaming" testing is a material aspect of the White House Executive Order. The Order describes AI red-teaming as a focused and dedicated testing activity designed to uncover flaws in an AI system. Red-teaming is a testing approach that has been used extensively for many years in relation to cybersecurity testing, including in the context of so called "ethical hacking". The NIST has defined a red-team in the cybersecurity testing context as follows: "A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment."[36] Google has defined red-teaming as follows: "Google Red

[31] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024], p. 2.

[32] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024], p. 4.

[33] , *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024]. pp. 13 -14.

[34] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024], p. 14.

[35] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.1 (ii).

[36] *Red Team (Definition)*, Computer Security Resource Center, Information Technology Laboratory, Glossary, National Institute of Standards and Technology Available from: https://csrc.nist.gov/glossary/term/red_team [Accessed January 16, 2024]. For further information on red-team testing in the computer nad information security area see for example Kraemer S.,Carayon P and Duggan R.(2004) *Red Team Performance for Improved Computer Security*, Proceedings of the Human Factors and Ergonomics Society Annual Meeting · September 2004. In English. Available from:

Team consists of a team of hackers that simulate a variety of adversaries, ranging from nation states and well-known Advanced Persistent Threat (APT) groups to hacktivists, individual criminals or even malicious insiders. The term came from the military, and described activities where a designated team would play an adversarial role (the "Red Team") against the "home" team."[37]

Based on the fact that the NIST has already looked to the field of cybersecurity red-teaming as a form of red-teaming that may be somewhat comparable to AI system red-teaming and that entities such a Google are also taking a similar approach it appears likely that when the Secretary of Commerce, acting through the Director of the NIST, works to establish AI system red-teaming guidelines per the instructions of the White House AI Executive Order the Secretary of Commerce and the NIST will continue to draw on the precedent and experiences of cybersecurity red-teaming for the development of such guidelines.

(iii) Dual-Use Foundation Model and Large Scale Computing Cluster Private Sector Reporting Requirements

A feature of the White House AI Executive Order that is likely to have the most immediate direct impact on the private sector is its instruction to the Secretary of Commerce that within a mere 90 days of the date of the Order the Secretary of Commerce must require companies developing or simply "demonstrating an intent to develop" potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records related to such models.[38] Although a significant portion of the White House AI Executive Order is aimed at instructions to government agencies which impact the manner in which the government itself will function, this dual use foundation model reporting requirement is aimed directly at the private sector.

The Order bases the President's power to create such an obligation directly on the private sector not on the powers invested in the President under the US Constitution, but rather on the Defense Production Act (DPA).[39] The Defense Production Act provides the President with broad authority over the US private sector in matters relating to national defense. The DPA was enacted during the administration of President Harry S. Truman in the context of US involvement in the Korean War. However, the DPA itself is based in a conceptual sense on the First War Powers Act of 1940 and Second War Powers Act of 1942, which gave the President broad authority to regulate industry during World War II.[40] Gradually over the years the US Congress has expanded the concept of national defense as defined in the DPA.[41]

---

https://www.researchgate.net/publication/228792785_Red_Team_Performance_for_Improved_Computer_Security [Accessed January 16, 2024].

[37] Fabian D., (2023) *Google's AI Red Team: the ethical hackers making AI safer*. [online] Available from: https://blog.google/technology/safety-security/googles-ai-red-team-the-ethical-hackers-making-ai-safer/ [Accessed January 17, 2024].

[38] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2 (i).

[39] Defense Production Act of 1950, as amended, 50 U.S.C. 4501 et seq.(2018) SI. United States. In English. Available from: https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim [Accessed January 17, 2024].

[40] First War Powers Act, 1941 (H.R. 6233, P.L. 77-354, 55 Stat. 838) (1941) SI. United States. In English. Available from: https://tile.loc.gov/storage-services/service/ll/uscode/uscode1946-00405/uscode1946-004050a009/uscode1946-004050a009.pdf [Accessed January 17, 2024] and Second War Powers Act, 1942 (S. 2208, P.L. 77-507, 56 Stat. 176) (1942) SI. United States. In English. Available from: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-1999-title50a-node230&edition=1999 [Accessed January 17, 2024].

[41] *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress* (2023), Congressional Research Service. United States. In English. Available from: https://sgp.fas.org/crs/natsec/R43767.pdf [Accessed January 17, 2024].

Under the White House AI Executive Order "dual-use foundation models are defined as follows: "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".[42] The following are provided as examples of such risks in the Order: "substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons", "enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks" and "permitting the evasion of human control or oversight through means of deception or obfuscation".[43]

Under the dual-use foundation model reporting requirements of the Order private sector entities are obligated to report on an ongoing basis on (1) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, (2) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and (3) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on the NIST red-team guidance discussed above and a description of any steps the entity has taken to meet safety objectives.[44]

The White House AI Executive Order also requires the Secretary of Commerce to mandate that that entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster.[45] There is debate, however, as to whether using compute threshold is an appropriate way to measure AI risk and therefore an appropriate trigger for reporting requirements. For example, in his testimony on the White House AI Executive Order before the US Congress' House Committee on Oversight and Accountability's Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Samuel Hammond, a senior economist for the Foundation for American Innovation, a group of technologists and policy experts focused on developing technology, noted: "The primary shortcoming of a compute threshold is that dangerous AI capabilities do not necessarily correlate with the scale of the compute used in training. …. Nonetheless, compute remains a reliable proxy for the performance of generalist

[42] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 3(k).

[43] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 3(k).

[44] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(a).

[45] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(ii). The Order also requires the Secretary of Commerce to develop the conditions for satisfaction of the definition of „large scale computing clusters" and provides a provisional set of conditions under such conditions can be developed by the Sectretary of Commerce. (Section 4.2 (b).)

AI models, and as such, the threshold is useful for picking out for special oversight the small number of companies attempting to create Artificial General Intelligence or AGI, while leaving the vast majority of AI research and development unscathed."[46]

(iv) Instructions Regarding United States IaaS Providers (i.e., Cloud Providers)

The White House AI Executive Order states that the President has found "that additional steps must be taken to deal with the national emergency related to significant malicious cyber-enabled activities".[47] In this context the Order requires that within 90 days of the date of the Order the Secretary of Commerce must propose regulations requiring United States IaaS Providers (that is, cloud providers such as Amazon, Google and Microsoft) to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a so-called "training run").[48] These reports, states the Order, must include the identity of the foreign person and the existence of any training run of such a large AI model or other criteria defined by the Secretary of Commerce in regulations.[49] The Order also requires that within 180 days of the date of the Order, the Secretary of Commerce must propose regulations that require United States IaaS Providers to ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account from the foreign reseller.[50]

The Order states that the regulations developed by the Secretary of Commerce must include a requirement that United States IaaS Providers prohibit any foreign reseller of their United States IaaS Product from providing those products unless such foreign reseller submits to the United States IaaS Provider a report, which the United States IaaS Provider must provide to the Secretary of Commerce, detailing each instance in which a foreign person transacts with the foreign reseller to use the United States IaaS Product to conduct a training run.[51]

These reporting requirements must be detailed in regulations that are to be proposed by the Secretary of Commerce. The requirements to a certain extent track the recommendations related to US cloud service providers set forth in the conclusions of the International Security Advisory Board (ISAB), a Federal Advisory Committee that provides the Department of State

---

[46] Hammond S., (2023) *Written Testimony of Samuel Hammond Senior Economist, Foundation for the American Innovation (FAI) Before the U.S. House Oversight Subcommittee on Cybersecurity, Information Technology, and Government Innovation*, United States. In English. Available from: https://cdn.sanity.io/files/d8lrla4f/staging/8147e2f9605ecae0296fbbbf35ef7ae4a8647ed9.pdf [Accessed January 17, 2024]

[47] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(c).

[48] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(c) (i).

[49] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(c)(i).

[50] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(d).

[51] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.2(c)(ii).

with advice on international security matters, as set forth in its October 31, 2023 Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins (the "ISAB AI Report").[52] The ISAB AI Report noted that US based cloud service providers are not currently required to identify and monitor entities using their advanced AI capabilities and that a higher level of awareness of who is using significant levels of AI cloud service provider computational power would be beneficial in broader AI safety and security efforts.[53] In this context the ISAB AI Report argued for a "Know Your Customer" ("KYC") regulatory framework for cloud service providers similar to that which exists in the financial services industry.

Should the regulations to be developed by the Secretary of Commerce come into force they would place a significant new compliance and reporting obligation on United States IaaS Providers as well as foreign resellers, similar to the additional compliance burdens placed on financial service entities via the financial services KYC regulatory requirements. Any such regulations in seeking to fulfill the goal of combatting malicious AI enhanced cyber-enabled activities could inhibit the competitive position of United States IaaS Providers vis-à-vis non-United States IaaS Providers.

(b) Instructions to Secretary of Energy

(i) Nuclear, Nonproliferation, Biological, Chemical, Critical Infrastructure, and Energy-Security Threats

The White House AI Executive Order states that within 270 days of its issuance the Secretary of Energy must develop tools to examine AI abilities to create content that could create nuclear, nonproliferation, biological, chemical, critical infrastructure, and energy-security threats.[54]

In the context of the relationship between AI and nuclear, nonproliferation, biological, chemical, critical infrastructure, and energy-security threats it is useful to consider the conclusions set forth in the ISAB AI Report. Within the subject of nuclear weapons and proliferation the ISAB AI Report focused more on the potential uses of AI to detect potential proliferation rather than for AI's potential use to create additional national security threats. In particular, the ISAB AI Report found that there exist new techniques that use big data and AI to detect early warnings of emerging nuclear weapons programs via examination and analysis of advances in civilian, dual-use, and weapons-related nuclear science and technology, and

[52] *Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins* (2023) United States. In English. Available from: https://www.state.gov/wp-content/uploads/2023/11/ISAB-Report-on-AI-and-Associated-Technologies_11172023-Accessible.pdf [Accessed January 17, 2024].

[53] *Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins* (2023) United States. In English. Available from: https://www.state.gov/wp-content/uploads/2023/11/ISAB-Report-on-AI-and-Associated-Technologies_11172023-Accessible.pdf [Accessed January 17, 2024], p. 34.

[54] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.1 (b).

through detection of the intent to change from civilian energy use to weapons use.[55]

With regard to AI and biological and chemical threats, the ISAB AI Report provides that the application of AI could enable the potential abuse of machine learning techniques for synthesizing harmful pathogens, chemicals, and other malicious products and that the dual-use nature of AI presents new challenges for those who assess national security risks associated state-sponsored biological and chemical weapons programs, and actions by non-state actors.[56]

7.2.2 Critical Infrastructure, Cyberdefense and Chemical, Biological, Radiological and Nuclear Weapons Threats

(a) Protecting Critical Infrastructure

The Order specifies that within certain stated deadlines various Federal institutions must take certain steps related to AI and the protection of critical infrastructure and cybersecurity. The Order utilizes the definition of "critical infrastructure" set forth in the USA Patriot Act of 2001. The USA Patriot Act, put into place following the September 11, 2001 terrorist attacks on the US, defines "critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[57] For example, the Order requires that Federal agencies and other entities with authority over critical infrastructure assess and report on risks related to the use of AI in critical infrastructure sectors, including how AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks and requires such entities to consider ways to mitigate these vulnerabilities.[58] The Order also states that without 180 days of its issuance the Secretary of Homeland Security must incorporate as appropriate the NIST AI Risk Management Framework into relevant safety and security guidelines for use by critical infrastructure owners and operators.[59]

(b) Cybersecurity and Cyberdefense

The Order requires that within 150 days of the date of the Order, the Secretary of the Treasury must issue a public report on best practices for financial institutions to manage AI-specific

---

[55] *Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins* (2023) United States. In English. Available from: https://www.state.gov/wp-content/uploads/2023/11/ISAB-Report-on-AI-and-Associated-Technologies_11172023-Accessible.pdf [Accessed January 17, 2024], p. 2.

[56] *Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins* (2023) United States. In English. Available from: https://www.state.gov/wp-content/uploads/2023/11/ISAB-Report-on-AI-and-Associated-Technologies_11172023-Accessible.pdf [Accessed January 17, 2024], p. 21-22.

[57] USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e), Section 1016(e) (2001) United States. In English. Available from: https://corpuslegalis.com/us/code/title42/critical-infrastructures-protection [Accessed January 17, 2024].

[58] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.3(a)(i).

[59] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], , Section 4.3(a)(iii).

cybersecurity risks.[60] In a report issued by the International Monetary Fund in August 2023 titled "Generative Artificial Intelligence in Finance: Risk Considerations" (the "IMF AI Fintech Report") a number of these cybersecurity risks in the financial services sector related to Generative AI such as ChatGPT were discussed.[61] The IMF AI Fintech Report noted, for example, that Generative AI could be used to generate more sophisticated phishing messages and emails or better enable malicious actors to impersonate individuals or organizations, leading to increased identity theft or fraud.[62] The IMF AI Fintech Report noted that Generative AI could be subject to "data poisoning" attacks which attempt to influence AI models at the training stage by adding special elements to the training data set and thereby seeking to undermine training accuracy or to hide malicious actions that wait for special inputs and also to "input attacks" which seek to influence the AI models during operation.[63]

(c) Chemical, Biological, Radiological and Nuclear Weapons Threats

The Order requires certain government agencies to take steps related to the potential use of AI to increase chemical, biological, radiological, or nuclear ("CBRN") weapons threats to the US. The Order highlights the need to focus on the use of AI in relation to biological weapons threats.[64] For example, the Order requires that within 120 days of its issuance the Secretary of Defense (1) assesses ways in which AI can increase biosecurity risks, including risks from generative AI models trained on biological data, and makes recommendations on how to mitigate these risks; (2) consider the national security risks associated with the use of data and datasets, especially those associated with pathogens and omics studies, that the government hosts, generates, funds the creation of, or otherwise owns, for the training of generative AI models, and makes recommendations on how to mitigate the risks , and (3) assesses the ways in which AI applied to biology can be used to reduce biosecurity risks.[65] The Order also requires that within 270 days of its, the Chief Data Officer Council must develop initial guidelines for performing security reviews which include reviews to identify and manage the potential security risks of releasing Federal data that could aid in the development of CBRN.[66]

---

[60] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.3(ii).

[61] Shabsigh G. and Bachir Boukherouaa E. *Generative Artificial Intelligence in Finance: Risk Considerations* (2023) International Monetary Fund, FinTech Note. United States. In English. Available from: file:///C:/Users/boonet/Downloads/FTNEA2023006%20(2).pdf [Accessed January 17, 2024].

[62]Shabsigh G. and Bachir Boukherouaa E. *Generative Artificial Intelligence in Finance: Risk Considerations* (2023) International Monetary Fund, FinTech Note. United States. In English. Available from: file:///C:/Users/boonet/Downloads/FTNEA2023006%20(2).pdf [Accessed January 17, 2024] p. 10.

[63] Shabsigh G. and Bachir Boukherouaa E. *Generative Artificial Intelligence in Finance: Risk Considerations* (2023) International Monetary Fund, FinTech Note. United States. In English. Available from: file:///C:/Users/boonet/Downloads/FTNEA2023006%20(2).pdf [Accessed January 17, 2024] p.10.

[64] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.4.

[65] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.4(a)(ii).

[66]*Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.7(a).

7.2.3 Synthetic Content

The Order places a significant emphasis on the government's approach to information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI - that is, so called "synthetic content".[67] In particular, the Order establishes steps for developing a framework for identifying and labelling synthetic content produced by the government or on its behalf. For example, the Order requires that within 240 days of the date of its issuance, the Secretary of Commerce must submit a report identifying the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for authenticating content and tracking its provenance; labelling synthetic content, such as using watermarking; (iii) detecting synthetic content; (iv) preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual); (v) testing software used for the above purposes; and (vi) auditing and maintaining synthetic content, that within 180 days of submitting such report the Secretary of Commerce must develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures and that within 180 days of the development of such guidance the Director of the White House Office of Management and Budget must "for the purpose of strengthening public confidence in the integrity of official United States Government digital content" issue guidance to government agencies for labelling and authenticating synthetic content that they produce or publish.[68]

The concept of creating regulations of label AI generated content has gained significant traction in the US in recent months. The purpose of such a label could be to indicate that content was generated using AI and to show that the content could mislead viewers.[69] For example, at the US Senate AI related hearing held on May 16, 2023 referred to above the issue of AI content labelling was discussed. At this hearing Altman, the CEO of Open AI, and Senator Richard Blumenthal had the following exchange:

Senator Blumenthal: "My question let me begin with you Mr. Altman, is should we consider independent testing labs to provide scorecards and nutrition labels or the equivalent of nutrition labels packaging that indicates to people whether or not the content can be trusted, what the ingredients are, and what the garbage going in may be, because it could result in garbage going out?"

Sam Altman: "Yeah, I think that's a great idea. I think that companies should put their own sort of, you know, hear the results of our test, of our model before we release it. Here's where it has weaknesses, here's where it has strengths but also independent audits for that are,

---

[67] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 3 (ee).

[68] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 4.5(a), (b) and (c).

[69] Eastwood B., *How should AI-generated content be labeled?* (2023); MIT Management Sloane School. United States. In English. Available from: https://mitsloan.mit.edu/ideas-made-to-matter/how-should-ai-generated-content-be-labeled [Accessed January 17, 2024].

are very important."[70]

7.2.4 AI Related Intellectual Property Issues

The Order initiates several steps to being the process of clarifying the relationship between content generated by AI and intellectual property ownership and related AI/intellectual property issues. For example, the Order requires that within 120 days of the date of the Order, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO) must publish guidance to USPTO patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process.[71] The guidance once published will likely have a significant impact on the debate of the relationship between AI assisted content and intellectual property. Questions which could be resolved by such guidance include whether AI can be considered an inventor or creator within the existing IP regulations; IP protection for AI algorithms and software; issues related to rights concerning the underlying training data and data inputs, and how the distinction between human creation and machine creation should be established.[72]

8. CONCLUSIONS

To a significant extent the White House AI Executive Order can be viewed as the formal start of the Biden Administration's intense focus to move US regulations on AI forward. Much of the Order consists of instructions to governmental agencies and other governmental entities to develop guidance and draft regulations for further review. Specific deadlines are set in the Order for much of the development of such guidance and draft regulations so such development is likely to take place fairly quickly. However, the precise content of such guidance and draft regulations, whether such regulations ever come into force, and if such regulations do come into force, their impact, is yet to be seen.

The area of the Order relating to dual-use foundation model and large scale computing cluster private sector reporting requirements is one that will have the most immediate impact on the private sector as those reporting requirements are mandated by the Order to be put in force within 90 days of the date of the Order.

To the extent that certain provisions of the Order relate solely to how the Federal government itself should conduct its activities vis-à-vis AI it is important to keep in mind that AI related actions required of Federal agencies will still impact non-government entities. This is the case because government agencies as purchasers of goods and services from the private sector will seek to impose contractual obligations on private-sector government contractors which comply with AI related regulatory governmental obligations. Hence, private sector government contractors will need to have in place operational frameworks which are compliant with such regulations, or at least do not cause the government entities with which they are contracting to not be in compliance with the AI related regulations applicable to such

[70] *Transcript of US Senate Judiciary Subcommittee Hearing on Oversight of AI* (2023) United States. Tech Policy.Press United States. In English Available from: https://www.techpolicy.press/transcript-senate-judiciary-subcommittee-hearing-on-oversight-of-ai/ [Accessed January 16, 2024].

[71] *Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), United States. In English. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [Accessed January 16, 2024], Section 5.2(c)(i).

[72] See *The WIPO Conversation on Intellectual Property and Artificial Intelligence* for further information. World Intellectual Property Organization. United States. In English. Available from: https://www.wipo.int/about-ip/en/artificial_intelligence/conversation.html [Accessed January 17, 2024].

governmental entities. In addition, the Federal government's approach to AI as eventually mandated combined with such associated compliance with private sector government contractors may serve as examples for other private sectors companies, whether or not they are government contractors, looking to establish an approach to using and working with AI.

Given the NIST's role is establishing the NIST AI Risk Management Framework, one of the most practical pieces of guidance to be issued by the US government related to AI, and the Order's instructions to the Secretary of Commerce, acting through the Director of the NIST, to establish guidelines to promote consensus industry standards for developing and deploying safe, secure, and trustworthy AI systems it is likely that that within the US government the NIST will going forward continue to play a substantial role in the future development of guidance and regulations related to AI. In addition, it is likely that the NIST will, in the context of developing such guidance and regulations, further look to the prior work of the ISO and the IEC, both non-governmental international organizations, associated with AI related standards, as the NIST did when drafting the NIST AI Risk Management Framework.

The Order places substantial focus on matters related to AI's potential impact on national security. This approach is understandable given the risks posed by AI in this area. The Order's looking to rough precedents, such as the precedent of the use of red-teaming in cybersecurity to serve as an example for red-teaming AI models and the precedent of KYC procedures now in use in the financial services sector serving as models for the establishment of KYC-type provisions for use by United States IaaS Providers is understandable and useful.

Overall, one must also keep in mind the inherent weaknesses of all Executive Orders – i.e., that they can be overridden by subsequent Presidential Administrations or by an Act of Congress and that they can be challenged in court on the basis of a President having exceeded the scope of Presidential authority. These inherent weaknesses, combined with the fact the White House AI Executive Order is largely a series of instructions to governmental entities to develop guidance and draft regulations, means that the actual impact of the White House AI Executive Order is largely yet to be seen. In addition, given the combination of these weaknesses and the US Congress' interest in the area of the regulation of AI as was demonstrated by, among other events, the May 16, 2023 Senate Hearing on AI, it is likely that the US Congress will not cease its activities related to AI in deference to Order but rather will continue to look closely at the possibility of regulating AI through the creation of Act focusing on AI. The EU's push to regulate AI through the EU AI Act may also act as a catalyst for the US Congress to move forward with an Act regulating AI so that the US may continue to claim a leadership role in the area of AI regulation. In addition, the EU AI Act's targeted risk based approach to the regulation of AI may, as was discussed in the May 16, 2023 Senate Hearing on AI, serve as a model for any future US Congressional action.

LIST OF REFERENCES

[1] *Executive Order14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence 2023*, United States. In English. Available from: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House; [Accessed January 14, 2024].

[2] Committee on Physical, Mathematical, and Engineering Sciences; Federal Coordinating Council for Science, Engineering, and Technology; Office of Science and Technology Policy, Office of Science and Technology Policy. (1994) *High Performance Computing & Communications: Toward a National Information*

Infrastructure. Washington, D.C., p. 1. In English. Available from: https://www.nitrd.gov/pubs/1994supplement/NITRD_Supplement-1994.pdf [Accessed January 16, 2024].

[3] National Academies of Sciences, Engineering, and Medicine. (1994) *Interim Report on the Status of the High Performance Computing and Communications Initiative*. Washington, DC: The National Academies Press. In English. Available from: https://nap.nationalacademies.org/read/10525/chapter/1 [Accessed January 16, 2024].

[4] National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee. (2016) *The National Artificial Intelligence Research and Development Strategic Plan.* Washington, D.C. In English. Available from: https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf [Accessed January 16, 2024].

[5] *Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence.* (2019) United States. In English. Available from: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence [Accessed January 16, 2024].

[6] *National Artificial Intelligence Initiative Act of 2020.* (2020) United States. In English. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6216/text [Accessed January 16, 2024].

[7] *Blueprint for an AI Bill of Rights.* (2022) United States. In English. Available from: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [Accessed January 16, 2024].

[8] *The US Bill of Rights, Constitution of the United States of America*. (1791). United States. In English. Available from: https://www.archives.gov/founding-docs/bill-of-rights-transcript [Accessed January 16, 2024].

[9] *European Commission White Paper On Artificial Intelligence – A European Approach to Excellence and Trust*. (2022) In English. Available from: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en [Accessed January 16, 2024].

[10] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023). National Institute of Standards and Technology, U.S. Department of Commerce, United States. In English. Available from: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) [Accessed January 16, 2024].

[11] *Transcript of US Senate Judiciary Subcommittee Hearing on Oversight of AI* (2023) United States. Tech Policy.Press In English Available from: https://www.techpolicy.press/transcript-senate-judiciary-subcommittee-hearing-on-oversight-of-ai/ [Accessed January 16, 2024].

[12] 47 U.S.C. 230 - Protection for private blocking and screening of offensive material (1996). United States. In English. Available from: 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu) [Accessed January 16, 2024].

[13] *European Commission Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence. Laying Down Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts* (2021) Available from: The Act | EU Artificial Intelligence Act [Accessed January16, 2024].

[14] *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI* (2023), EU Parliament Press release. In English. Available from Artificial Intelligence Act: deal on

comprehensive rules for trustworthy AI | News | European Parliament (europa.eu)[Accessed January 16, 2024].

[15] *Presidential Transitions: Executive Orders* (2020) Congressional Research Service, United States. In English. p 2. Available from: Presidential Transitions: Executive Orders (fas.org) [Accessed January 16, 2024].

[16] Newland E., (2015) *Executive Orders in Court*, The Yale Law Journal, Volume 124, Number 6, April 2015. Available from: https://www.yalelawjournal.org/note/executive-orders-in-court [Accessed January 16, 2024].

[17] ISO - About us and What IEC does (2024). In English. Available from: ISO - About us [Accessed January 16, 2024].

[18] *Using and referencing ISO and IEC standards to support public policy* (2024), ISO and IEC. In English. Available from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100358.pdf [Accessed January 16, 2024].

[19] *ISO/IEC 22989:2022, Information Technology Artificial intelligence concepts and terminology*, ISO. In English. Available from Publicly Available Standards (iso.org) [Accessed January 16, 2024].

[20] *Red Team (Definition)*, Computer Security Resource Center, Information Technology Laboratory, Glossary, National Institute of Standards and Technology Available from: https://csrc.nist.gov/glossary/term/red_team [Accessed January 16, 2024].

[21] Kraemer S.,Carayon P and Duggan R.(2004) *Red Team Performance for Improved Computer Security*, Proceedings of the Human Factors and Ergonomics Society Annual Meeting. September 2004. In English. Available from: https://www.researchgate.net/publication/228792785_Red_Team_Performance_for_Improved_Computer_Security [Accessed January 16, 2024].

[22] Fabian D., (2023) *Google's AI Red Team: the ethical hackers making AI safer*. [online] Available from: https://blog.google/technology/safety-security/googles-ai-red-team-the-ethical-hackers-making-ai-safer/ [Accessed January 17, 2024].

[23] Defense Production Act of 1950, as amended, 50 U.S.C. 4501 et seq.(2018) SI. United States. In English. Available From: https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim [Accessed January 17, 2024].

[24] First War Powers Act, 1941 (H.R. 6233, P.L. 77-354, 55 Stat. 838) (1941) SI. United States. In English. Available from: https://tile.loc.gov/storage-services/service/ll/uscode/uscode1946-00405/uscode1946-004050a009/uscode1946-004050a009.pdf [Accessed January 17, 2024]

[25] Second War Powers Act, 1942 (S. 2208, P.L. 77-507, 56 Stat. 176) (1942) SI. United States. In English. Available from: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-1999-title50a-node230&edition=1999 [Accessed January 17, 2024].

[26] *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress* (2023), Congressional Research Service. United States. In English. Available from: https://sgp.fas.org/crs/natsec/R43767.pdf [Accessed January 17, 2024].

[27] Hammond S., (2023), *Written Testimony of Samuel Hammond Senior Economist, Foundation for the American Innovation (FAI) Before the U.S. House Oversight*

Subcommittee on Cybersecurity, Information Technology, and Government Innovation, United States. IN English. Available from: https://cdn.sanity.io/files/d8lrla4f/staging/8147e2f9605ecae0296fbbbf35ef7ae4a8647ed9.pdf [Accessed January 17, 2024]

[28] *Final Report of the International Security Advisory Board (ISAB) on the Impact of Artificial Intelligence and Associated Technologies on Arms Control, Nonproliferation, and Verification issued to US Undersecretary for Arms Control and International Security Bonnie D. Jenkins* (2023) United States. In English. Available from: https://www.state.gov/wp-content/uploads/2023/11/ISAB-Report-on-AI-and-Associated-Technologies_11172023-Accessible.pdf [Accessed January 17, 2024].

[29] USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e), Section 1016(e) (2001) United States. In English. Available from: https://corpuslegalis.com/us/code/title42/critical-infrastructures-protection [Accessed January 17, 2024].

[30] Eastwood B., *How should AI-generated content be labeled?* (2023),MIT Management Sloane School. United States. In English. Available from: https://mitsloan.mit.edu/ideas-made-to-matter/how-should-ai-generated-content-be-labeled [Accessed January 17, 2024].

[31] *The WIPO Conversation on Intellectual Property and Artificial Intelligence* for further information. World Intellectual Property Organization. United States. In English. Available from: https://www.wipo.int/about-ip/en/artificial_intelligence/conversation.html [Accessed January 17, 2024].

[32] Peng S. Lin C. and Streinz T. (Eds.) (2021) *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration*. Cambridge- Cambridge University Press.

[33] Iansiti M and Lakhani K. (2020) *Competing in the age of AI: strategy and leadership when algorithms and networks run the world*. Boston, Massachusetts: Harvard Business Review Press.

[34] Siebel T. (2019) *Digital Transformation: survive and thrive in an era of mass extinction*. New York: Rosetta Books.

[35] Koulu R. (2020) *Proceduralizing control and discretion: Human oversight in artificial intelligence policy*, Maastricht Journal of European and Comparative Law, Volume 27, Issue 6, Available from: https://journals.sagepub.com/doi/full/10.1177/1023263X20978649 [Accessed January 17, 2024].

[36] Diamandis P. and Kotler S. (2020), *The Future Is Faster Than You Think*, New York: Simon & Schuster.

[37] Henry Kissinger H., Schmidt E. and Daniel Huttenlocher D. (2021) *The Age of AI*, London: John Murray (Publishers).