U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

November 3, 2022

The Honorable Haley Stevens
Chair
Subcommittee on Research
and Technology
Committee on Science,
Space and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Randy Feenstra
Ranking Member
Subcommittee on Research
and Technology
Committee on Science,
Space and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairwoman Stevens and Ranking Member Feenstra:

Please see below my response to the Question for the Record I received after my testimony in front of your Subcommittee for the September 29 hearing, "Trustworthy AI: Managing the Risks of Artificial Intelligence."

Question: In October 2022, the White House issued the *Blueprint for an AI Bill of Rights*, which is comprised of "a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence." From the U.S. Chamber's perspective, how does the Administration's approach through the AI Bill of Rights differ from NIST's approach through the AI Risk Management Framework to bolster innovation and transparency in trustworthy AI? Do you find the Administration's approach helpful to building consumer confidence and trustworthiness of AI systems?

OSTP's and administrations' release of the AI Bill of Rights does not help foster innovation, transparency, and trustworthiness in AI. Furthermore, we see that the release of the AI Bill of Rights creates potentially significant conflicts with the congressionally mandated NIST AI Risk Management Framework for the following reasons.

I. Creating Uncertainty and Conflicting Frameworks

The "blueprint" puts unnecessary uncertainty in the current domestic and international work taking place to develop "trustworthy AI." As the United States continues to develop and refine the Congressionally mandated NIST Risk

Management Framework, and our international counterparts such as Israel, Singapore, Japan, Canada, and the EU continue to look to work on these matters, it is essential for the United States government to lead by example with one specific plan to help move domestic and international policy in a direction which helps American businesses, continue innovation, and to allow for the opportunity to address trustworthy AI holistically and thoughtfully.

The AI Bill of Rights has done the exact opposite, as our allies are now confused about the stance and direction the United States is taking on current and future policy around the development of AI. For example, it has been reported[1] that the United States recently provided critical feedback to the EU on its forthcoming EU AI Act. That feedback includes the United States support for "individualized risk assessments.[2]" However, this explicitly contradicts the AI Bill of Rights, which advocates for a broader regulatory approach.

II. Lack of Transparency

The adoption of the AI Bill of Rights was not a transparent process, which harms businesses and the American public's trust to be a part of these critical conversations. Although the "Blueprint" highlights Organizations from which OSTP met and received feedback, we would like to emphasize that the process lacked the openness and transparency necessary to obtain sufficient stakeholder input about these complex issues. Furthermore, the only request for information from OSTP regarding the "AI Bill of Rights" was related to biometrics[3] and not artificial intelligence. Without the necessary stakeholder feedback on matters the blueprint addresses, OSTP fails to create a complete record of the use of the technology. This contradicts the work that has transpired at NIST with the Risk Management Framework. NIST, at this time, has done three workshops and four RFIs around the development of the RMF. The timing of the release of the Bill of Rights, given its transparency deficiencies, is disappointing in light of the congressionally mandated stakeholder driven approaches at NIST and the National AI Advisory Committee.

III. Unworkable Definitions

---

[1] https://www.euractiv.com/section/digital/news/the-us-unofficial-position-on-upcoming-eu-artificial-intelligence-rules/

[2] https://www.euractiv.com/section/digital/news/the-us-unofficial-position-on-upcoming-eu-artificial-intelligence-rules/

[3] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-onpublic-and-private-sector-uses-of-biometric-technologies

Definitions within the blueprint do not help harmonization. While defining terms is a critical step, the definitions used within the "Blueprint" could potentially harm the United States' ability to identify the appropriate and necessary lexicon among like-minded international allies. For example, the definition of "Automated System" is comprehensive and the use of the phrase "includes, but not limited to," leads to unnecessary uncertainty around what is an "Automated System." Any definition of an Automated System must be clearly defined. This counter to the NIST Framework uses a Congressionally enacted definition, which aligns with the OECD's AI Principle.

IV. Concerns with Audits

The Blueprint's call for independent evaluations by third-party auditors also raises concerns. There are no concrete standards and metrics for auditing Artificial Intelligence systems. The Blueprint's call to allow "Independent Evaluators, such as…journalists…third-party auditors" to be "given…unfiltered access to the full system" is pointless at a time when independent evaluations of AI systems continue to lack any standardization. NIST Risk Management Framework runs counter to this part of the blueprint, as the Framework is about developing internal consciences about addressing and mitigating bias instead of opening businesses and organizations to unfiltered access. Furthermore, NIST is producing the upcoming playbook, which provides suggested actions, references, and documentation guidelines for stakeholders to achieve outcomes[4]."

V. Conflating Data Privacy with Algorithmic Policy

The blueprint conflates data-privacy with Artificial Intelligence: The Blueprint lists "Data Privacy" as one of the five principles of the Blueprint. While we wholeheartedly agree that data is a significant part of Artificial Intelligence, it is essential to highlight that the two are distinctly different issues. Data Privacy has long been understood to be how an individual's data is used and shared. Where Artificial Intelligence is when the data is used in conjunction with algorithms that learn from that data to do a specific assigned task, it is essential not to conflate these two issues, as the nuances and complexities in each case are distinctly different.

The Chamber also takes exception with the term "surveillance" when referring to the use of data broadly, as the A.I. Bill of Rights appears to do. In its current Advanced Noticed of Proposed Rulemaking related to "commercial surveillance," the FTC utilizes a definition of commercial surveillance that effectively captures all data analysis in business.[5] This term is used pejoratively without considering technology's benefits for

[4] https://pages.nist.gov/AIRMF/

[5] 87 Fed. Reg. 51277 "For the purposes of this ANPR, ''commercial surveillance'' refers to the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that

things like the affordability of goods and services, financial inclusion, public safety, and improving health outcomes.

VI. Call For Codification

The Chamber is deeply concerned that the "blueprint" intends to influence state and local government to model legislation after its principles and recommendations. This was stated as one of the goals in a blog post by OSTP during the reveal of the blueprint, which stated that "policymakers can codify these measures into law or use the framework and its technical companion to help develop specific guidance on the use of automated systems within a sector.[6]"

The call to codify principles that have not been fully vetted, discussed and analyzed on their specific merits and economic impact will lead to unintended consequences for those communities. The use of the blueprint to validate efforts to regulate the use of Algorithms is already occurring. For example, the Attorney General of the District of Columbia authored a blog post highlighting that he "supports the white house AI Bill of Rights[7]," which "includes Core Aspects of His Office's Bill[8]." It is essential that communities have the necessary conversation and dialogue about using technology to build understanding and trust. Instead, the codification of the AI Bill of Rights could lead to unnecessary regulations, which never received the necessary discussion and analysis.

Sincerely,

Jordan Crenshaw
Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

---

information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first."

[6] https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

[7] https://oag.dc.gov/release/ag-racine-supports-white-house-ai-bill-rights

[8] https://oag.dc.gov/release/ag-racine-supports-white-house-ai-bill-rights