



November 21, 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20510

RE: Victoria Espinel's Responses to Additional Questions for the Record

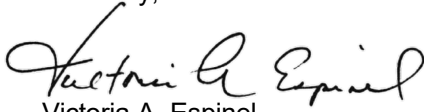
Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on October 18, 2023, to testify at the hearing entitled "Safeguarding Data and Innovation: Setting The Foundation For The Use Of Artificial Intelligence."

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thank you for your help, and please let me know if you have any questions.

Sincerely,


Victoria A. Espinel

Attachment

Attachment—Additional Questions for the Record

The Honorable Russ Fulcher

1. Your industry includes software creators, database firms, and I imagine, data storage companies. You have discussed the role and responsibilities of those who develop software, as well as “deployers” who use software in various business, entertainment, gaming, and other areas. You’ve talked about the different roles of developers and deployers. Why should regulation address both of those roles and how do these different companies work together to address concerns created by an AI system?

Legislation should recognize the different roles of companies that develop and deploy AI systems because these companies will have access to different types of information and will be able to take different actions to mitigate risks. Developers are the companies that design, code, or produce an AI system, such as a software company that develops an AI system for speech recognition. In contrast, deployers are the companies that use an AI system, such as a bank that uses an AI system to make loan determinations.

Legislation should assign different obligations to these different companies, to reflect the different actions they can take to identify and mitigate risks of an AI system. For example, the developer of an AI system is well positioned to describe features of the data used to train that system, the system’s known limitations, and its intended use cases, but it generally will not have insight into how the system is used after it is purchased by another company and deployed. In contrast, a company that deploys an AI system is well positioned to understand how the system is actually being used, what type of human oversight is in place, and whether there are complaints about how the system works in practice. Developers should make available to deployers relevant information about the capabilities, limitations, and intended uses of an AI system. Legislation must recognize these different roles in order to assign obligations that reflect a company’s role in developing or deploying an AI system.¹ The concept of role-based responsibilities is not unique to AI, and it is considered best practice in privacy and security legislation worldwide.

2. You focused on the importance of managing risks associated with AI systems. How are companies using the AI Risk Management Framework published earlier this year by the National Institute of Standards and Technology (NIST)? Should the US government look to that RMF more broadly, including setting standards for procurement?

The NIST AI Risk Management Framework (RMF) is an important mechanism for identifying and mitigating risks, and we encourage organizations to adopt it. The RMF is flexible and can be adapted to entities of all sizes. Companies are using the RMF to assess risks by mapping the practices identified in the RMF to their existing controls, to identify where gaps exist so that they can develop additional risk mitigation practices where needed. The RMF is also enhancing companies’ governance of AI issues. The RMF is an excellent model that both companies and the U.S. government should adopt. Incorporating the NIST RMF as part of procurement for high-risk uses of AI would help establish the US government as a market leader on responsible AI, embracing best practices for managing AI risks, and holding federal contractors to the same standard.

¹ See BSA, *AI Developers and Deployers: An Important Distinction*, available at <https://www.bsa.org/files/policy-filings/03162023aidevdep.pdf>.

3. Tell me about the importance of a federal preemption, and of the ability to meet better a national standard when it comes to not just the privacy and controls on data that supports AI software programs, but a national standard on generative and other AI programs?

National laws on privacy and AI are critical to avoiding a patchwork of obligations and will help create consistency across the United States. This consistency makes it easier for businesses of all sizes across all industries to use technology to grow. Countries that support the responsible adoption of AI will be best positioned to see the growth in jobs and economic prosperity the technology offers. Consumers should have clear expectations about what rights they have, and companies should have a clear understanding of what their obligations are across state lines. A single U.S. approach to these issues will also be important for the United States to have a strong international voice on the best approach to regulating AI.

The Honorable Jeff Duncan

1. What defines high-risk uses of AI vs. everyday AI? How should Congress make a distinction between high-risk AI and other applications?

High-risk uses of AI are those that lead to consequential decisions – decisions that determine the eligibility for and result in the provision or denial of housing, credit, employment, education, access to physical places of public accommodation, healthcare, or insurance. These are the uses that have the most significant impact on an individual’s important life opportunities.

Legislation should focus on high-risk uses so that it does not unnecessarily sweep in low-risk uses of AI. For example, there are many everyday uses of AI by consumers and businesses that present few risks to individuals and create significant benefits. These include consumer-facing services that identify when someone forgets to attach a document to an email, or business-facing uses that can help companies improve cybersecurity, optimize manufacturing, or strengthen their logistics planning.²

The Honorable Darren Soto

On September 12, 2023, in testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, you encouraged Congress “to adopt legislation that creates meaningful guardrails for high-risk uses of AI.” Specifically, you testified that such legislation must require companies to complete the following:

- **Establish risk management programs to identify and mitigate risks across AI systems**
- **Conduct annual impact assessments for high-risk uses of AI, and**
- **Publicly certify that they have met these requirements.**

Given the rapidly evolving threats and challenges associated with AI, the requirements outlined in your testimony offer a prudent first step in establishing an appropriate legislative framework. My only concern with this approach, however, is the absence of any required independent assurance over a company’s risk management and impact assessment methodologies.

² See BSA, Everyday AI for Consumers, available at <https://www.bsa.org/files/policy-filings/08012023aiconsumers.pdf>, and Everyday AI for Businesses, available at <https://www.bsa.org/files/policy-filings/08012023aibusiness.pdf>.

I believe the independent verification of risk management processes not only complements your proposal but further enhances organizational transparency and accountability. To this end, I have a few related questions:

1. Ms. Espinel, have you considered the potential benefits of requiring an internal audit function to provide objective assurance over certain AI-related functions (i.e. risk management programs and impact assessments)?

Yes. An important part of a risk management program is evaluating and refining the processes in place to identify and mitigate risks. This internal analysis helps strengthen AI governance within companies. It also helps companies adapt more easily to emerging risks. Conducting this review internally allows companies to engage in a more rigorous assessment of its governance processes and AI systems, without creating concerns that may arise in external contexts about the potential disclosure of trade secrets and other commercially-sensitive information.

2. Ms. Espinel, how many of your member companies currently utilize internal audit as a resource in identifying and mitigating risks associated with AI? What barriers are preventing widespread adoption of organizational internal audits?

Internal impact assessments have increasingly become integral parts of risk management programs, including those of BSA member companies. We think legislation should require companies to adopt risk management programs and to conduct impact assessments if they develop or deploy AI systems for high-risk uses. We do not believe that there are barriers to adopting these practices. On the contrary, impact assessments are an existing tool that is widely used in other contexts, such as privacy. We believe impact assessments would create an important new accountability tool for high-risk uses of AI and can be implemented by companies of all sizes.