INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

October 9, 2024

The Honorable Alejandro Mayorkas,
Secretary, United States Department
of Homeland Security

Dear Secretary Mayorkas,

I am writing as Chairman of the National Institute of Standards and Technology (NIST) Information Security and Privacy Advisory Board (ISPAB). By statute, the ISPAB is charged with advising NIST, the Secretary of the Department of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal Government information systems as well as the development of security and privacy standards.

At its meeting on July 17-18, 2024, the Information Security and Privacy Advisory Board (ISPAB) received two briefings related to the responsible and secure development, deployment, and evaluation of artificial intelligence (AI). Reva Schwartz from NIST presented an update on Assessing Risks and Impacts of AI (ARIA), and Dr. Tyson Brooks of the National Security Agency (NSA) presented an update on the new Artificial Intelligence Security Center (AISC). There was also brief discussion of the Cybersecurity and Infrastructure Security Agency (CISA) Joint Guidance on Deploying AI Systems Securely. The Board understands that there is a great need and demand for guidance on how to responsibly develop and deploy AI, both within and outside the federal government, and commends the work that is being done.

At the same time, it is the Board's view that the U.S. government would benefit from coordinating AI safety efforts across agencies. Doing so could prevent duplicated development efforts, harmonize recommendations across agencies, and streamline stakeholders' process for using this guidance. For example, we would like to avoid a future scenario in which stakeholders must consult multiple documents from different agencies to obtain the required information regarding AI safety guidelines. Worse yet, we would like to avoid scenarios in which stakeholders receive inconsistent advice from different agencies (not to mention guidance developed by industry standards organizations, such as the OASIS Coalition for Secure AI (COSAI).

To this end, the U.S. government may benefit from mapping out the scope of work happening across these new AI centers and similar guidance-generating entities across the government and seeking coordination to the maximum extent feasible. The Board recommends NIST lead a cross-agency collaboration to ensure that efforts to develop AI safety and security standards and guidelines are being coordinated and integrated. Specifically, we suggest the following:

1. In cases where guidance is being developed for a specific community (e.g., critical infrastructure or defense) we suggest the leads of each effort to articulate which parts of the guidelines are specific to that community, and which parts are domain-agnostic.
2. For guidelines that are domain-agnostic, we suggest ensuring that the recommendations from different agencies are consistent with one another.
3. For international standards development impacting AI regulation and guidance, we suggest coordination pre- and post-meetings to prevent conflicting input to standards development.
4. Finally, we suggest that the involved agencies jointly release a document explaining the differences between existing guidance documents and directing end users to the appropriate one(s) based on their needs.

Once again, we thank the NSA, NIST, and CISA for their ongoing efforts to promote AI safety within the U.S. government and beyond. We look forward to seeing the impacts of this important work.

Thank you very much.

Sincerely,

Steven B. Lipner
Chair
Information Security and Privacy Advisory Board

CC: Dr. Laurie Locascio, Under Secretary of Commerce for Standards and Technology and Director, National Institute of Standards and Technology (NIST), and
Shalanda D. Young, Director, Office of Management and Budget (OMB)