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

Shalanda D. Young
Director,
Office of Management and Budget

Dear Ms. Young,

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.

The development of standards, at both the national and international level, requires deep understanding of technical and business needs, strategic and often diplomatic national interests, and thoughtful engagement to bring about a successful result that endures. When done correctly, standards that reflect US interests create opportunities that advance US technical interests and American technologies around the world.

The ISPAB appreciates NIST efforts to develop standards for the US federal government, particularly those that focus on cybersecurity, privacy, and Artificial Intelligence (AI). It also recognizes that incorporating NIST recommendations into international standards strengthens the security of those standards and makes it easier for industry to meet security requirements. Additionally, standards often reflect strategic national security interests and focus on standards and standards competition should be a strategic priority, as captured in the U.S. Government's National Standards Strategy for Critical and Emerging Technology (USGNSSCET). The ISAPB recommends the NIST consider international standards development a priority for continued and sustained participation, particularly in technologies and issues related to cybersecurity and privacy in critical and emerging technologies such as AI. The ISPAB understands that participation in international standards development can be costly in time and travel expenses but believes that the importance of standards justifies making their support a budget priority.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

The USGNSSCET calls out standards engagement efforts across the USG and around the world. It is a welcome call, given the challenge of maintaining US engagement in standards development efforts. Standards are often developed in lengthy, drawn-out processes that require travel and periods of multiple days' engagement in order to make progress. While some nations are aggressively pursuing standards as a means of international influence, the USGNSSCET recognizes the importance of strong U.S. engagement on standards. It is clear to the ISPAB that increased coordination of international standards efforts—between USG agencies, between USG and industry, and between USG and foreign governments—will only strengthen those standards and therefore improve US cybersecurity. The ISPAB recommends that NIST take the lead on such coordination, in support of the US's industry-led standards ecosystem.

As NIST faces increasing demands to lead the country's engagement in international standards and decreasing budgets, we are concerned that participating in international standards organizations may be one of the first initiatives to face the chopping block because travel expenses and participation fees are easy to isolate and cut in a given budget cycle. Given the impact of NIST's standards leadership on the entire Federal Government as well as national competitiveness, we recommend that OMB work with NIST to evaluate the budgetary needs and explore how other agencies who are stakeholders in the country's standards strategy can contribute to NIST's standards efforts.

It is critical to US economic and national security that US industry continue their strong support of international standardization efforts. However, and as noted above, standards participation is costly and time consuming, which makes it difficult for small- and medium-sized businesses to engage. Such businesses are often at the forefront of research, development, and pre-standardization efforts in critical and emerging technologies. The ISPAB recommends NIST alleviate the burden of standards engagement to these companies through NIST-led consortia that complement, support, and supplement the important work that occurs in similar industry-led consortia. Such consortia lower the barrier to entry for U.S. and allied businesses interested in meeting security standards requirements. These consortia can also support Recommendation 2D from the PCAST Cyber Physical Resilience Report to host more meetings in the United States in order to increase U.S. participation in standards development efforts.

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),