From: Stephanie Hall <SHall@nam.org>
Sent: Thursday, October 24, 2019 3:50 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Good afternoon,

Please find attached here comments from the National Association of Manufacturers on the NIST Privacy Framework: Preliminary Draft Comments.

Please feel free to reach out with any questions or concerns.

Best,

Stephanie

Stephanie Hall

National Association of Manufacturers

Director, Innovation Policy

Email: shall@nam.org

Direct: (202) 637-3072

NAM Facebook | Twitter | Instagram | LinkedIn | YouTube

Stephanie Hall
Director
Innovation Policy

October 24, 2019

Katie McFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

RE: NIST Privacy Framework: Preliminary Draft Comments

On behalf of the 14,000 members of the National Association of Manufacturers (NAM), the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states, the NAM submits these comments on the National Institute of Standards and Technology (NIST) Request for Comment (RFC) on the Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Preliminary Draft).

Manufacturing employs more than 12 million men and women, contributes over $2 trillion to the U.S. economy annually, has the largest economic impact of any major sector and accounts for more than three-quarters of all private-sector research and development in the nation. The NAM is the powerful voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States.

Manufacturers are developing innovative products and transforming the manufacturing process with the latest technologies. Data continues to be a critical source and biproduct of these breakthroughs and developments as modern manufacturing evolves. The Internet of Things (IoT) is continuing to transform manufacturing through billions of connected devices and advanced wireless infrastructure that allow for the transmission of vast amounts of data. Connected shop floors are creating data that industry is harnessing to improve efficiency, manage production activities, streamline repairs and safeguard plant security. Additionally, connected products utilize data to transform the customers' experience in countless ways.

Our nation's manufacturers support NIST's efforts to develop a voluntary, risk-based Privacy Framework that advances individuals' privacy while promoting U.S. innovation and industrial competitiveness. Like the NIST Cybersecurity Framework, a Privacy Framework provides an important benchmark and guide for companies seeking to improve and secure their operations. The Preliminary Draft Privacy Framework includes provisions that can be used by organizations to accomplish that same goal, and the NAM welcomes the opportunity to provide these comments.

Continued economic growth in the manufacturing sector will be positively impacted by a federal policy approach to data privacy if it fosters innovation and accounts for the diverse ways that organizations are integrating data into their operations and products. Ongoing innovation requires flexibility, and any federal action on data privacy must be carefully balanced and

thoughtfully implemented without sacrificing opportunities for economic leadership and progress.

The NAM supports NIST's outcomes-based approach to the Privacy Framework that avoids prescriptive recommendations and practices for an organization. By focusing on outcomes, organizations have the flexibility to develop risk-based privacy practices suitable to their business models. An outcomes-based approach to privacy is necessary to account for the diverse ways data is used across different sectors and companies. The federal approach to data privacy must be flexible enough to account for various types of data, including consumer data, business-to-business data and data from digitized shop floors.

Manufacturers design and build security and privacy into their systems and products, and it is often an extensive process to adjust those systems and products in the face of evolving data regulations. We appreciate that the Preliminary Draft includes a section on how to apply the Privacy Framework throughout the information system development life cycle. We urge NIST to continue to develop a Framework that accounts for this distinction and can be applied to a wide range of sectors and technologies.

A NIST Privacy Framework should anticipate the constantly evolving nature of technology and be flexible enough to work for the data-intensive innovations of the future. Manufacturers are leading the development and application of emerging technologies, including automation, Artificial Intelligence, and quantum computing, among other developments in advanced manufacturing. The federal government should be mindful of current and future uses of data and embrace policies that promote U.S. progress and leadership in these emerging technologies.

Our companies are entrusted with vast amounts of data through diverse business interactions with customers, vendors, suppliers and governments. They understand that safeguarding privacy, protecting information and building consumer trust is a critical responsibility. The Preliminary Draft's inclusion of terminology to clarify the variety of entities and roles within the data processing ecosystem is helpful both to organizations working to manage privacy risk and to stakeholders considering and developing data privacy policies and laws.

NIST's Privacy Framework Request for Information identified the need for the Privacy Framework to be compatible with existing domestic and international privacy approaches. This continues to be a top priority for manufacturers. Within the Core of the Privacy Framework, the "Govern-P" function provides steps for organizations to create a governance structure that allows them to prioritize and customize privacy efforts consistent with the organization's business needs and risk management approach. One aspect of developing this governance structure includes "identifying legal/regulatory requirements." This is an important part of an organization's effort to manage privacy risks. However, patchwork requirements and unpredictable regulatory changes on data privacy are currently undermining the ability of organizations to identify these requirements and manage privacy risks with the certainty they need. NIST should consider ways to provide expertise and guidance to elected leaders and policymakers at federal, state and local levels to help prevent conflicting laws and requirements.

A patchwork of state laws on consumer privacy stalls innovation by creating a regulatory burden that distracts from the development of next generation technologies and products. State-by-state privacy requirements create conflicts for manufacturers, their operations and their processes due to the interstate nature of data flows. Congress and the Administration should develop a federal privacy policy that provides clarity and certainty for manufacturers. Federal

privacy legislation should pre-empt state privacy regulations to resolve conflicting requirements in different states. A national approach to data privacy will strengthen businesses while supporting consumers.

In addition to providing regulatory harmony within the United States, a federal privacy framework should be interoperable with global privacy frameworks such as the EU's General Data Protection Regulation. This is necessary to ensure U.S. manufacturers with global operations and international data flows are not stymied by conflicting international frameworks. Manufacturers appreciate regulatory certainty in global business enterprises because 95 percent of the world's consumers live outside the United States. A confusing and inconsistent regulatory privacy regime deters U.S. manufacturers from seeking access to new markets or from delivering the best, most advanced products to their customers in different markets.

As NIST continues to develop a Privacy Framework, manufacturers support a data privacy approach that provides flexibility for innovation, addresses domestic and global inconsistencies in privacy regulations and advances U.S. economic growth and technological leadership. The NAM respectfully submits these comments for NIST's consideration.

Comments submitted via email to privacyframework@nist.gov by:

Stephanie Hall
Director of Innovation Policy
National Association of Manufacturers
733 10th Street NW, Suite 700
Washington, DC 20001