January 14, 2019

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

Re: Request for Information on Developing a Privacy Framework, Docket Number 181101997-8997-01

Dear Ms. MacFarland:

BSA | The Software Alliance appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology's Request for Information ("RFI") on Developing a Privacy Framework.[1] BSA is the leading advocate for the global software industry.[2] Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing and artificial intelligence ("AI") products and services. In the United States, software contributes $1.14 trillion to U.S. GDP and supports 10.5 million jobs, with an impact in each of the 50 states and across a range of industries.[3] As global leaders in the development of data-driven products and services, BSA members prioritize the protection of consumers' personal data, and they understand that protecting privacy is a key part of building consumer trust.

BSA supports NIST's efforts to develop a voluntary enterprise risk management framework, which could lead to a useful operational tool that allows companies to strengthen privacy best practices. NIST's leadership in developing the Cybersecurity Framework demonstrated that a voluntary, consensus-driven approach can produce highly valuable results; the Cybersecurity Framework has significantly enhanced organizations' ability to identify and address security risks, and the process and guiding principles behind this earlier effort should serve as the model for developing the Privacy Framework.

BSA also supports federal legislation establishing uniform national privacy standards based on certain best practices and envisions a continuing, important role for the Privacy Framework under such legislation. In particular, federal privacy legislation should implement best practices that increase the transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and

---

[1] Developing a Privacy Framework, 83 Fed. Reg. 58,624 (Nov. 14, 2018) ("RFI").

[2] BSA's members include: *Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.*

[3] *See* Software.org: The BSA Foundation, *The Growing $1 Trillion Economic Impact of Software*, at 5 (Sept. 2017), *available at* https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes. The same objectives should govern *any* consumer privacy framework, legislative or otherwise.

This comment responds to the RFI's question regarding the overarching considerations related to the framework's attributes. Part I of the comment suggests further elaboration and next steps with regard to three of the seven Privacy Framework attributes that the RFI proposes. Part II recommends that NIST add an attribute, Promoting Innovation, to recognize the many benefits of data use and the incorporation of such benefits in existing privacy standards and frameworks, including BSA's own privacy framework.

I. Furthering the NIST Privacy Framework's Minimum Attributes

BSA supports including each of the seven objectives that the RFI identifies as minimum attributes for the privacy framework.[4] Notably, NIST's recognition of the need to avoid prescriptive approaches will be critical. Below, we address three of the other attributes – compatibility with other privacy approaches (*i.e.*, interoperability); adaptability to different organizational, business, and technical situations; and clearly defined audiences – which are also particularly important to ensuring that the Privacy Framework maximizes its utility to businesses. We also suggest one additional attribute for NIST to consider: The privacy framework should be designed to aid innovation.

A. Interoperability

The RFI rightly proposes to ensure that the Privacy Framework "take[s] advantage of existing privacy standards, methodologies, and guidance" and is "compatible with and support[s] organizations' ability to operate under different domestic and international legal or regulatory regimes."[5] Interoperability along these different dimensions will be key to the Privacy Framework's success. While the Privacy Framework will be a voluntary tool, its utility would be significantly enhanced if it not only is developed in light of industry standards and legal requirements but also provides a structure that helps organizations map the Framework to requirements that apply to them. Accordingly, BSA recommends that NIST continue to develop the interoperability attribute, beginning with the February 2019 workshop. Two specific steps would be helpful in this regard.

As an initial step, NIST should identify existing technical, legal, and regulatory standards that are significant to stakeholders. Developing a comprehensive assessment of this landscape will be necessary to achieve the ultimate objective of interoperability. In addition, some existing standards, such as the Cybersecurity Framework and the ISO 27000 series, are likely to be sources of enterprise risk management practices and security standards that NIST can leverage to develop the Privacy Framework as a whole. Referring to existing standards would also help reduce fragmentation of privacy operations and enhance national and global interoperability.

---

[4] The attributes are: (1) consensus-driven and developed through an open, transparent process; (2) use of common and accessible language; (3) adaptable to different organizations, technologies, sectors, and uses; (4) risk-based, outcome-based, voluntary, and non-prescriptive; (5) readily usable as part of an organization's existing broader risk management strategies; (6) compatible with other privacy approaches; and (7) a living document capable of being updated as technologies and approaches change. *See* RFI, 83 Fed. Reg. at 56,825.

[5] *See* RFI at 56,825 (stating that the "Privacy Framework should be consistent with, or reinforce, other risk management efforts within the enterprise, recognizing that privacy is one of several major areas of risk that an organization needs to manage").

We also recommend that NIST seek input on the level, or levels, of interoperability that organizations may achieve under the Privacy Framework. Organizations will want to determine how the Privacy Framework maps to the various standards and requirements that they must follow. Incorporating interoperability benchmarks could help organizations determine how to allocate their resources in order to put the Privacy Framework into practice, as well as communicate the value of the Privacy Framework throughout their organizations. Both features would encourage use of the Privacy Framework.

B. Adaptability

We underscore the importance of the RFI's recognition that the Privacy Framework "should be scalable to organizations of all sizes, public or private, in any sector, and operating within or across domestic borders."[6] NIST should strive to ensure that the Privacy Framework is useful to organizations with many different sizes, business models, and sectoral and geographic legal requirements. At the same time, it is critical to observe the markedly different data use and privacy considerations – including starkly difference legal frameworks – in the public and private sectors.[7] Making the Privacy Framework applicable under these various contextual factors will be key to limiting its applicability to specific technologies, sectors, or business models. Avoiding a prescriptive approach is therefore paramount.

C. Define Audiences and Organizational Roles

BSA strongly supports the use of "common and accessible language" to make the Privacy Framework "broadly understandable by a wide audience, including senior executives and those who are not privacy professionals."[8] Although plain language is a necessary element of reaching broad audiences, it is not sufficient. It is critical to identify and define intended audiences for the Privacy Framework, which, in turn will help NIST and stakeholders to understand the roles of various actors within organizations, their responsibilities, and their concerns. Soliciting participation in public workshops by individuals with different responsibilities relating to privacy could help NIST ensure that the Privacy Framework's substance and style reach a broad audience.

II. Promoting Innovation as a Minimum Attribute of the Privacy Framework

As NIST seeks to enable organizations to better assess and manage privacy risks, it should also be cognizant of the backdrop in which these issues arise – companies' development of products and services that are providing significant economic growth and societal improvements. These benefits include the application of artificial intelligence to solve challenges in healthcare, fraud detection, cybersecurity, and other areas.

The RFI focuses extensively on privacy risk and does not refer explicitly to innovation and other benefits of data use. Other risk management frameworks, including NIST's draft *Risk Management Framework for Information Systems and Organizations*[9] and BSA's Privacy

[6] RFI at 56,825.

[7] *See id.* (indicating NIST's intent to make the Privacy Framework applicable to the public sector).

[8] *Id.*

[9] NIST, Draft Special Publication 800-37 (May 2018), at 44, 49.

Framework,[10] explicitly address the need to consider beneficial uses of data in conjunction with risks. To remain in step with these and other frameworks, and to provide a more comprehensive guide to enterprise risk management decisions, the Privacy Framework should include an attribute on promoting innovation. Such an approach would not only achieve the dual aims of enhancing privacy protection and aiding innovation, but it would also increase the operational utility of the framework.

As an example, BSA's Privacy Framework recognizes that the use of personal data should be consistent with consumers' expectations while also enabling companies to pursue legitimate business interests.[11] The BSA framework articulates ten principles that would outline a general plan for strong consumer protections; strong organizational practices that support these protections; and consistent, robust enforcement.[12] However, an organization's application of some of these principles in practice will depend on, among other things, how it uses data and what benefits these uses create. For example, BSA's principles of Transparency and Consumer Control are inherently context-specific. NIST could bring significant value to stakeholders by exploring ways to provide guidance for such individualized considerations through the Privacy Framework.

In addition, the role and importance that organizations assign to specific data practices also may depend on how the Privacy Framework incorporates innovation. For example, deidentification and other privacy-preserving techniques can enable innovation and reduce certain privacy and data security risks. The Privacy Framework should also contemplate how these kinds of practices aid innovation and provide guidance that organizations can use to inform decisions about which techniques to employ in light of their innovation and privacy-enhancing benefits.

***

NIST's development of a privacy framework comes at a critical time when many stakeholders are assessing, and reassessing, how best to protect consumer privacy. BSA appreciates NIST's contribution to this broader dialogue and is pleased to serve as a resource as the development of the Privacy Framework continues.

Sincerely,

Shaundra Watson

Shaundra Watson
Director, Policy
BSA | The Software Alliance

[10] *See generally* BSA | The Software Alliance, Privacy Framework (released Sept. 12, 2018), https://www.bsa.org/~/media/Files/Policy/BSA_2018_PrivacyFramework.pdf.
[11] *Id.*
[12] *Id*.