Cisco Systems, Inc.

www.cisco.com

January 14, 2019

Submitted to privacyframework@nist.gov

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

RE: Request for Comment on "Developing a Privacy Framework"

I am writing on behalf of Cisco Systems, Inc. in response to your request for comment on the development by the National Institute of Standards and Technology (NIST) of a Privacy Framework. We thank NIST for spotlighting the important issue of privacy engineering and the need for further rigor around both privacy and security by design. As noted below, the NIST Cybersecurity Framework (CSF) has proved the power of the model—i.e., a standards-based, process-oriented framework for managing risk. While the subjects of privacy and security are in many ways distinct, there are sufficient areas of overlap such that coordination in risk-management efforts within and between organizations is necessary. We, therefore, urge NIST, wherever feasible, to adopt an approach consistent with the CSF when developing the Privacy Framework, which will maximize both interoperability and uptake of the two frameworks.

Cisco is the world leader in building the infrastructure of the global internet and has provided a significant portion of the switches, routers, and other equipment used by U.S. telecommunications service providers and enterprises. Our past is rooted in connectivity, and our future is being built around it. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. We, therefore, agree with your assessment that more must be done to accelerate the advancement of technology engineered with privacy and security in mind, by design, and by default.

We thank NIST for its leadership not only in spotlighting concerns around how to advance the state of privacy engineering, but also for spearheading the effort to develop a Privacy Framework. We believe that this initiative will: 1) raise awareness of privacy engineering concepts; 2) increase use of risk-based approaches for managing privacy risks; and 3) highlight areas where additional standards development work is necessary.

It is encouraging that NIST is leading this effort given both its experience as a convener of multi-stakeholder efforts to address complex technology problems and its sustained commitment to: 1) open and transparent mechanisms for policy development; 2) leveraging voluntary,

Cisco Systems, Inc.

www.cisco.com

consensus-based standards as required by longstanding U.S. law and policy;[1] and 3) process-oriented approaches to manage risk. This combination is best suited to driving widespread adoption of the results in the marketplace.

In addition to modeling the effort to develop a Privacy Framework on the processes used to develop the CSF, NIST should strive to achieve the greatest degree of interoperability with the CSF feasible. The power of the CSF framework stems from the manner in which it provided organizations a consistent way to: identify risks requiring management; select controls available to manage the risks; and assess their maturity at managing risks against a target state. It would be unnecessarily confusing to differ from that approach in the development of the forthcoming Privacy Framework without some significant justification.

Accordingly, NIST should start work on a Privacy Framework with the baseline assumption that the core functions—i.e., identify, protect, detect, respond, recover—are equally applicable as they were to the CSF. Wherever feasible, the method used to identify and apply relevant controls should be similar. If that turns out to be true, NIST's efforts to build a Privacy Framework will yield an approach capable of rapid adoption by organizations already using the CSF. At the same time, it will focus future standards development efforts on gaps identified through the process of assembling a privacy-specific set of "informative references."

As noted above, Cisco agrees with NIST that development of a Privacy Framework can help spur the market to proactively engineer privacy controls into technologies. We fully expect that the resulting approach will have a positive impact on data protection and privacy much in the same way that the development of the CSF drove adoption of risk-based processes for cybersecurity. While this effort is intended to manage risks that are distinct from those addressed in the Cybersecurity Framework, we recommend that the new document be developed with the explicit intent of enabling interoperability between privacy and security risk management wherever possible.

Again, we thank NIST for its important leadership in this area and we look forward to continued engagements with the Department of Commerce on this and other matters relating to privacy and security engineering.

Best wishes,

Eric Wenger,
Director, Cybersecurity and Privacy Public Policy
1/14/2019

[1] See: National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and Office of Management and Budget (OMB) Circular A-119, as revised.