Cybersecurity Coalition

DRAFT

January 14, 2019

Submitted to privacyframework@nist.gov

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"

The Cybersecurity Coalition ("Coalition") submits this comment in response to the Request for Information ("RFI") issued by the National Institute of Standards and Technology ("NIST") on November 14, 2018 regarding the development of a framework that can be used to improve organizations' management of privacy risk (the "Privacy Framework").[1] The Coalition looks forward to working with NIST to encourage the promotion of cybersecurity activities that can help organizations manage privacy risk arising from the collection, storage, use, and sharing of individuals' information. As noted below, while this effort is intended to manage risks that are distinct from those addressed it the Cybersecurity Framework, we recommend that the new document be developed with the explicit intent of enabling interoperability between them whereever possible.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices and voluntary standards throughout the global community.

The Coalition appreciates the opportunity to provide these comments and participate in this important discussion. Though our members are acutely focused in the security space, we welcome the opportunity to help develop and encourage privacy best practices in areas where privacy and security overlap. We recognize that NIST has already provided specific guidance on cybersecurity best practices through its Framework for Improving Critical Infrastructure Cybersecurity, which was most recently updated in April 2018 (the "Cybersecurity Framework").[3] As a result, we do not suggest that the security principles outlined in the Cybersecurity Framework should be

[1] *See* 83 Fed. Reg. 56824-56827 (Nov. 14, 2018).
[2] The views expressed in this comment reflect the consensus views of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, *see* www.cybersecuritycoalition.org.
[3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 (April 16, 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

rehashed entirely in the Privacy Framework. However, the Coalition believes that robust security practices and controls are crucial for protecting individuals' privacy, and therefore, cybersecurity tools should serve as an integral part of a successful Privacy Framework. To that end, the Coalition supports the advancement of a reasonable, risk-based Privacy Framework in which effective security principles are incorporated as a key component—and is designed to enable consistent risk management across both data protection and cybersecurity.

I. High-Level Goals for the Privacy Framework

Employ a Risk and Outcome-Based Approach. Effective privacy solutions require an integrated approach to data security, including the use of best practices that promote interoperability and data sharing to enable effective threat analysis. Privacy and security frameworks must promote technology neutral, risk-based solutions that encourage accountability, innovation, and efficiency. Privacy laws around the world, including Europe's General Data Protection Regulation ("GDPR"), encourage the development of such risk and outcome-based frameworks.[4] The Privacy Framework should reflect this general approach, and should emphasize the importance of creating and advancing more specific, particularized privacy standards to build technical controls that can help enable a risk-based approach. The Coalition supports the development of a reasonable, risk-based Privacy Framework where robust security principles are included as a necessary and integrated part of the solution. The Coalition recommends a flexible approach explicitly modeled on the Cybersecurity Framework in order to accomplish this goal most effectively.

Clarify How the Cybersecurity Framework and Privacy Framework Should Work Together. Because security is a fair information practice principle, there are many areas in which organizations will need to consider privacy and security simultaneously. As a result, it is important that NIST clarifies how the Cybersecurity Framework and Privacy Framework should work together to inform entities' data practices. The Cybersecurity Framework is powerful because it gives organizations a consistent way of assessing risks to be managed, identifying controls and standards available to manage those risks, and understanding their own maturity and ability to manage such risks. The Coalition therefore recommends that NIST begin its efforts to develop a Privacy Framework by assessing the viability of using the Cybersecurity Framework as a general structural model for the Privacy Framework.

NIST should prioritize enabling organizations to easily implement the Cybersecurity Framework and Privacy Framework at the same time. To do so, NIST should work to highlight similarities and eliminate misalignments, including in terminology, between the two. The Coalition believes that NIST should adopt a general approach similar to the Cybersecurity Framework by delineating core functions, categories, subcategories, and informative references in

[4] Recital 76 of the GDPR states: "The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."

the Privacy Framework. Including the same structural elements in the Privacy Framework that already appear in the Cybersecurity Framework will: (1) encourage interoperability between the two frameworks, (2) yield a Privacy Framework capable of rapid adoption by organizations using the Cybersecurity Framework, (3) allow for a streamlined cross-mapping process between both frameworks, and (4) ensure that future efforts are focused on developing standards where gaps have been identified in order to effectively manage the risks associated with data protection and privacy. This is not to suggest that the actual functions and categories must necessarily be the same in both Frameworks, but only that the Privacy Framework should interoperate with the Cybersecurity Framework and adopt its general approach of utilizing core functions, categories, subcategories, and informative references.[5] Where it would be reasonable to map the terminology to that used in the Cybersecurity Framework, that approach should be preferred. Where differentiation is necessary, the reasoning should be explained and the distinctions made clear.

Our members, as well as our peers in the cybersecurity industry, process threat data from hundreds of millions of Internet points of presence, the local access points that allow users to connect to the Internet with their Internet Service Provider (ISP), to protect customers from cybersecurity attacks and support them to meet their privacy compliance obligations. These actions help protect the privacy of individuals' data by enabling companies to better secure their systems against potential data breaches and threats from hackers. The ability to gain operational insight into attack vectors, through the appropriate and responsible use of individuals' data, also enables the cybersecurity industry to continue to bring innovative solutions to the market that increasingly drive the ability to detect and defeat "zero day" attacks, which are attacks that have zero days between the time a vulnerability is discovered and the initial attack. Thus, the Privacy Framework should address and encourage the processing of individuals' data for security purposes. The ideal privacy approach will encourage good corporate behavior to protect data in accordance with recognized industry standards.

II. Areas to Consider to Properly Address Security in a Risk Management-Focused Privacy Framework

The Coalition recommends that the Privacy Framework address the following key areas, each of which incorporates critical security principles in order to bolster the ability of companies to effectively protect individuals' privacy by protecting access to their data.

Privacy and Security by Design. Privacy and Security by Design are principles that encourage companies to proactively consider privacy and security when developing products and services for the marketplace, as well as when implementing internal tools. Privacy and Security

[5] Where practicable, utiziling the same control sets as categories and subcategories and same informative references for these categories, would also be helpful to limit duplication or misunderstandings for organizations using both frameworks. For example, many of the categories in the "Identify" function in the Cybersecurity Framework may very well prove to be equally applicable to the Privacy Framework.

by Design means protecting data through proactive technology design. This proactive approach to designing technology is the most effective and efficient way to enable data protection, because the data protection strategies are integrated into the technology when it is created. The Coalition believes Privacy and Security by Design encourages accountability in the development of technologies, making certain that privacy and security are included as foundational components of the product and service development process. Building technology with privacy and security considerations integrated at the outset also helps to enable legitimate uses of data and moves the conversation beyond binary consent-only options. The Coalition advocates for the Privacy Framework to include proactive Privacy and Security by Design principles to enable the most effective end-to-end privacy and security technology solutions and to move beyond limiting, consent-only models.

Bases for Processing. The Coalition also urges NIST to encourage organizations to move beyond traditional notice and consent regimes when broaching the subject of how to address data privacy and security together. The Privacy Framework should, therefore, address the fact that processing individuals' data for security purposes is a key way to bolster data privacy. Thus, the Privacy Framework should highlight healthy organizational privacy practices, such as storing data only for as long as necessary and only for its intended purpose, to help ensure that the security and privacy of individuals' data is protected. The Privacy Framework also should promote bases for processing data that have been accepted in other legal regimes, including Legitimate Interests, a key part of the GDPR framework and one that explicitly recognizes the sort of risk and benefit analysis that NIST has championed in early discussions of the Privacy Framework.[6]

Information Sharing. As more digital devices are connected to the Internet, there will be an increased need for data and applications to be shared among devices and to be stored remotely (e.g. cloud), with augmented focus on the balance of performance, power management, and security. The move from device to cloud adds additional complexity to the data landscape. For there to be appropriate privacy protections for this data, there will need to be an increased focus on security of the networks, the gaps between and among clouds, and individual end devices. Like allowing any device to connect to a network, some device information (e.g. IP addresses) will need to be connected and processed for security purposes. It is important that this processing and sharing of information is recognized by the Privacy Framework as a necessary mechanism for protecting privacy by better securing data.

Additionally, the Privacy Framework should enable and encourage information sharing in an organization to organization context for security purposes. The Coalition believes that the key

[6] *See* General Data Protection Regulation, Article 6(1)(f); Recital 47 ("The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding . . . . the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned . . . .")

to empowering organizations to engage in more effective information sharing is to ensure that such organizations are assessing and managing the risks associated with handing data in a compatible manner. The Privacy Framework should help facilitate this interoperability by giving organizations common tools to identify areas of risk, identify controls for those risks, and assess implementation of the controls.

The Coalition broadly supports robust privacy and security mechanisms from a technical and process standpoint, but the overall system must also allow for and reinforce information sharing capabilities between companies and organizations when needed. Because myriad entities provide security solutions for different critical applications, including healthcare, the electric grid, fraud prevention, anti-money laundering, and other vital sectors, such entities need to share information in order to deliver solutions that go beyond network security and cybersecurity alone. The Privacy Framework should enable such information sharing by outlining how organizations can handle data in ways that are familiar to one another, so that greater interoperability between organizations working on common security threats may be achieved.

The Coalition believes privacy and security are necessary prerequisites for companies to comply with laws, to grow businesses and improve efficiencies, and for individuals to trust technology. Processing of device information (e.g. IP addresses) is necessary to connect to the Internet and to provide reasonable security for personal data. Likewise, sharing threat and other necessary information with respect to critical applications is an important tool for bolstering and enhancing privacy and security solutions on a macro level.

III. Conclusion

The Coalition is confident that the Privacy Framework will be an important tool for entities to use to better structure their organizational approaches to privacy and cybersecurity. We believe that a risk and outcome-based approach to the Privacy Framework will yield the best results, and we urge NIST to provide specific guidance to organizations about the ways in which the Privacy Framework and Cybersecurity Framework should work together. We recommend that the Privacy Framework adopt a privacy and security by design approach, promote legitimate interests as a basis for data processing, and include terms that help build interoperable capabilities for information sharing among entities. Privacy and security are of paramount importance to the companies that comprise the Coalition. The Coalition hopes that NIST will rely on our industry expertise to help build this useful Privacy Framework tool.

* * *

The Coalition appreciates the opportunity to submit these comments, and looks forward to continued collaboration with NIST as it continues its efforts to advance consumer privacy.

Respectfully Submitted,

DRAFT

The Cybersecurity Coalition

January 14, 2019

CC: Ari Schwartz, Venable LLP