December 5, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments – Privacy Methodology

Dear Mr. Sedgewick,

The attached comments are the result of discussions of representatives from a variety of industry sectors including automotive, communications, financial services, government contractors, and information technology products and services.

There is general agreement that: the Framework process is focused on critical infrastructure sectors; Executive Order 13636 mandates inclusion of a privacy methodology in the Framework; and Section 7(a) of the Executive Order mandates that the Cybersecurity Framework "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."

It is important that the Cybersecurity Framework be implementable and used. To that end, a privacy methodology should focus on the privacy issues directly and uniquely implicated by an organization's cybersecurity measures or controls. In this respect, not all cybersecurity measures or controls have privacy implications. As stated on page 28 of the Preliminary Cybersecurity Framework, "not all Categories give rise to privacy and civil liberties risks."

There is consensus that the privacy methodology included in the Preliminary Cybersecurity Framework should be narrowed and focused so that, like the rest of the Framework, it reflects consensus private sector practices. The attached submission accomplishes this approach. Subsequent versions of the privacy methodology can address issues as to which consensus does not yet exist.

Further, elsewhere in the Framework is where NIST should address measures and controls to protect personal information, including personal information that may be targeted as a means to access other assets within the organization, since such information is one of several types of important information to be protected by an organization's unified cybersecurity program.

To incentivize use of the Cybersecurity Framework, the privacy methodology must be clear and straightforward for the private sector to use. A privacy methodology that attempts to map privacy principles to most features of the Framework or to recommend open-ended and potentially burdensome practices (such as minimizing collection and storage of a very broad range of personal information) would be difficult for organizations to follow and risks discouraging organizations from committing to use the Framework. Organizations should be able readily to determine how to use the privacy methodology and whether they have incorporated its elements.

Finally, the privacy methodology should not overstate the availability or applicability of existing standards, given the degree to which this field is dynamic and requires innovation. It would chill use of the Framework for the privacy methodology to include the Fair Information Practice Principles (FIPPs) as applied to cybersecurity given the lack of consensus private sector standards in this regard. As stated on page 39 of the Preliminary Cybersecurity Framework, "There are few identifiable standards or best practices to mitigate the impact of cybersecurity activities o individuals' privacy . . . ."

Thank you for the opportunity to provide input into this process.

Harriet Pearson

Harriet P. Pearson
Partner
Hogan Lovells US LLP
55 13th Street, NW
Washington, D.C. 20004

harriet.pearson@hoganlovells.com

Attachment

Alternative Methodology to Protect Privacy for a Cybersecurity Program

Methodology to Protect Privacy for a Cybersecurity Program

This part of the Cybersecurity Framework presents a methodology to address the collection and use of protected information related to an organization's cybersecurity activities. This part does not extend or apply to commercial data activities outside of the cybersecurity context.

Securing personal information is an element of both cybersecurity as well as privacy programs overall, and is addressed in Appendix A (Framework Core) in a number of relevant categories such as Risk Assessment (RA), Risk Management Strategy (RM), Data Security (DS), Information Protection Processes and Procedures (IP), and Protective Technology (PT). Securing such information is therefore not addressed in this part.

The term "protected information" used in this part means "personal information that (i) is subject to security breach notification requirements, (ii) an organization is restricted by law from disclosing, (iii) an organization is required by law to secure against unauthorized access, or (iv) an organization voluntarily so designates."

Potential Privacy Considerations Related to Cybersecurity Activities	Organizational Privacy Measures and Controls
An organization's overall governance of cybersecurity risk should consider privacy implications of its cybersecurity program.	An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program. Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained. Process is in place to support compliance of cybersecurity activities with applicable privacy laws. Process is in place to assess implementation of the foregoing organizational measures and controls.
Approaches to identifying and authorizing individuals to access organizational assets and systems may raise privacy considerations.	Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection or use of protected information relating to identifiable individuals.
An organization's cybersecurity monitoring activities may raise privacy considerations.	Process is in place to conduct privacy review of an organization's cybersecurity monitoring activities
Information-sharing pursuant to cybersecurity activities may raise privacy considerations.	Process is in place to assess and address whether, when, how, and the extent to which protected information is shared outside the organization as part of cybersecurity information sharing activities.
The organization's cybersecurity awareness and training measures should include privacy considerations.	Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities. Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies.