Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	
	)	
Developing a Framework to Improve	**)**	**Docket No. 130909789–3789–01**
Critical Infrastructure Cybersecurity	**)**	

Comments of the Internet Commerce Coalition

on the Preliminary Cybersecurity Framework Released by the National Institute of Standards and Technology

The Internet Commerce Coalition (ICC) is comprised of leading Internet and e-commerce companies and trade associations, including Amazon, AOL, AT&T, Comcast, eBay, Google, Monster.com, Verizon, Tech America and US Telecomm Association. The ICC is pleased to submit comments on the Preliminary Cybersecurity Framework ("Framework") released by the National Institute of Standards and Technology (NIST). Our comments focus solely on Appendix B, the "Methodology to Protect Privacy and Civil Liberties" (the "Privacy Methodology").

We propose that NIST substitute for the current Privacy Methodology, the "Alternative Privacy Methodology to Protect Privacy for a Cybersecurity Program", that Harriet Pearson submitted to Adam Sedgewick, Information Technology Laboratory, National Institute of Standards and Technology (Dec. 5, 2013), available at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf ("Alternative Privacy Methodology") and also included at the end of these comments. This Alternative Privacy Methodology is the product of intensive work by a broad cross-section of private sector owners and operators of Critical Infrastructure, including the ICC and its members, and reflects current private sector privacy best practices in this area.

I. The Current Privacy Framework Should Be Replaced In Its Entirety

The ICC has serious concerns with regard to the lengthy Privacy Methodology that NIST issued for public comment.

A. The Framework Inappropriately Attempts to Apply Public Sector Standards to Private Sector Operations

Unlike most of the Framework Core, the Privacy Methodology would depart sharply from existing law and industry best practices. The Privacy Methodology takes as its starting point NIST Special Publication 800-53, Revision 4, Appendix J ("Appendix J"), a standard that was developed for the Government, not the private sector, and relates to requirements of the Federal Privacy Act, the Federal Government's privacy statute, which the White House 2012 report *Consumer Data Privacy In A Networked World* acknowledged governs the Federal Government's handling personal information, not private sector practices.[1] These standards have never been applied to the private sector and are a very awkward fit with private sector cyber security practices.

As NIST recognizes on page 39 of the Framework, "[t]here are few identifiable standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy." 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 using the Framework.

Instead, the Privacy Methodology should focus on privacy risks posed by specific

[1] *Consumer Data Privacy In A Networked World*, at 5, n.1.

cybersecurity functions rather than applying broader privacy requirements across functions described in Appendix A.

B. The Range of Personal Information Covered Is Too Broad

The Privacy Methodology goes far beyond incorporating privacy practices into an organization's cybersecurity program. If included in the Final Framework adopted, it would create uncertainty and discourage use of the Framework by private sector organizations.

The Privacy Methodology on its face appears to apply to the full spectrum of PII with repeated cross-references to NIST Special Publication 800-53, rev. 4, Appendix J. This definition goes far beyond the definitions of PII under existing laws and recent legislation. It would reach "information *which can be used to distinguish or trace an individual's identity* such as their name, social security number, biometric records, etc., alone, *or when combined with other personal or identifying information which is linked or linkable to a specific individual*." This range of PII is unworkable in the context of an organization's cybersecurity program, for example, by virtue of requiring "a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements."[2] These are rarely functions performed in conjunction with cybersecurity programs and would impair an organization's ability to defend against cyberattacks.

C. Overlap Between the Framework Core and The Privacy Methodology Should Be Eliminated

Securing data assets is already addressed in the Framework Core and personal information is just one of several types of information that should be protected under an organization's cybersecurity program. Addressing securing personal information under different standards in the Privacy Methodology is both unnecessary and confusing. For this reason, references to securing personal information outside of cybersecurity operations should be removed from the Privacy Methodology.

The Privacy Methodology contains unworkable data minimization requirements that would require organizations to use the bare minimum amount of PII necessary to carry out cybersecurity functions. This would chill legitimate cyber security practices that necessarily involve use of information about threats, for example, and would risk undermining cyber security.

The Privacy Methodology requires data minimization when an organization is collecting information in conjunction with detecting anomalies and events, minimizing disclosure when reporting breaches, and retaining only that which is "necessary" to a forensics investigation in responding to an event. By restricting an organization's use, retention, and sharing information on cyber incidents to only the PII and communications content that is necessary for detection, investigation, and response, the Privacy Methodology would require special privacy compliance measures that could impair security measures and increase the costs associated with adopting the Framework.

[2] OMB Memorandum 10-22.

In the absence of specific statutory cybersecurity liability protections designed to encourage Framework adoption, the data minimization and retention language in the Privacy Methodology would risk discouraging more rapid and wide-spread adoption of meaningful cybersecurity practices such as threat monitoring, defending against threats, and threat information sharing. It would prompt additional delays for legal reviews and assessments both in the context of an organization's threat response posture, and in the context of enterprise cybersecurity transactions, where protracted negotiations over the allocations of risks perceived to be posed by such requirements would not help the rapid delivery of cybersecurity solutions to market. Further, the inclusion of communications content in the Privacy Methodology is an unnecessary diversion from the Methodology's focus on privacy, as communications content can be necessary to identify malicious code, for example.

E. Lack of Standards or Consensus on Private Sector Civil Liberties Considerations Make Inclusion in the Framework Premature

Civil liberties protections are almost always an obligation on the government. Although individual companies may have internal policies in this area, there is no standard or consensus around how to protect civil liberties in the context of cybersecurity. Again, if the Framework proposes processes that are unclear, it will limit the adoption of the Framework.

The Privacy Methodology states that organizations should assess the impact on individuals' privacy and civil liberties especially when the containment of a threat involves closing public communications or data transmission systems. This language would add additional uncertainty in an already uncertain legal landscape. It is phrased broadly enough that it could be interpreted as declaring otherwise appropriate responses to security threat incidents resulting in a temporary disruption of service to be potentially unlawful impacts on privacy rights or civil liberties. Private sector communications companies have powerful market incentives not to disrupt service if at all possible when responding to cyber security incidents. Without corresponding statutory cybersecurity liability protections, such language would unnecessarily confuse the private sector and result in delaying rapid deployment and widespread adoption of effective cybersecurity strategies.

F. Accuracy Requirements Are Burdensome and Not Necessary

Further, the Privacy Methodology would require that organizations responding to a cybersecurity incident have policies on PII to ensure that is "collected, used, disclosed or retained" in accurate and complete form. This requirement, too, is excessive for many organizations and would create unnecessary costs for many organizations without a clear benefit.

II. NIST Should Adopt the December 5th Alternative Privacy Methodology

We recognize that the Administration is determined to include a privacy section in the final Framework. If it does so, it should adopt the Alternative Privacy Methodology discussed above. The ICC and several of its members worked extensively on the content of the Alternative Privacy Methodology and the ICC believes that it would focus appropriately on cyber security

activities that potentially may give rise to privacy considerations. The Alternative Privacy Methodology reflects a cross-sector consensus on how private sector organizations should address privacy in conjunction with cybersecurity activities.

The Alternative Privacy Methodology: 1) does not extend or apply to commercial data activities outside of the cybersecurity context; 2) applies to "protected information" rather than broadly defined PII; and 3) does not address civil liberties considerations , which are generally applicable in the context of government actions, more so than those of the private sector.

The Alternative Privacy Methodology is laid out in two columns. The first column lists "Potential Privacy Considerations Related Cybersecurity Activities" and the second column outlines high-level "Organizational Privacy Measures and Controls" that are process-based, rather than outcome-based. This approach will allow individual organizations to tailor their process to the unique circumstances of their business and legal considerations, such as applicable sectorial privacy regulation. However, the content listed under the columns could easily be incorporated directly into the Framework Core also.

The definition of the term "protected information" is drafted in a flexible manner that allows application by organizations within any industry sector regardless of regulatory status. It applies to "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." The ICC supports this definition in that it does not expand current law or create new expectations as is a concern with the NIST Privacy Methodology.

This language could either be included in a substitute Appendix B or in a section in the Framework Core.

III. Conclusion

For all these reasons, the ICC urges NIST to adopt the Alternative Privacy Methodology to the Privacy Methodology either as a standalone appendix to the Cybersecurity Framework or incorporate it into the narrative of the Framework Core.

Respectfully submitted,

s/ Sydney M. White
Counsel to Internet Commerce Coalition

December 5th Alternative Privacy 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 a 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.

Potential Privacy Considerations Related to Cybersecurity Activities	Organizational Privacy Measures and Controls
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.