THE **PROVIDENCE** GROUP

February 22, 2016

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Via email

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt,

We are writing on behalf of The Providence Group, a cybersecurity enterprise risk management consultancy that works with clients in a number of critical infrastructure sectors, including healthcare and utilities. We appreciate the opportunity to respond to the National Institute of Standards and Technology's (NIST) request for information to update its framework to reduce critical infrastructure cybersecurity risk.

We believe that the current framework's functions and categories are particularly useful for organizations to better understand their processes and procedures for developing or improving a cyber risk management plan. Additionally, we believe that the structure of the framework is well designed to integrate with an organization's approach to other operational risks and disaster management plans.

However, we believe that the current framework leads to some confusion regarding the appropriate and essential role of risk management at the organizational level (Tier 1), especially in the development of a cybersecurity risk management strategy. This confusion stems from the language used in the framework that appropriately describes the process of risk management and the Appendix A implementation reference documents that focus on security controls at the Information Systems level (Tier 3).

The NIST Cybersecurity Framework includes in its discussion of risk management the identification of threats, establishment of risk tolerance and governance of cybersecurity risk. Importantly, it also mentions that it is flexible enough to be used with a variety of risk management processes and identifies some relevant examples. Unfortunately, the framework is not explicit that the cybersecurity risk management process, especially the initial critical process of Risk Framing, is an organizational (Tier 1) activity incorporating the most senior level executives in the corporate suite. This is an important distinction because only those leaders can appropriately make decisions on what risks will be tolerated, strategy decisions and business trade-offs that might increase cybersecurity risk and allocate resources that will be directed toward cybersecurity.

Recommendation to Update the Framework

We suggest that the framework be updated to include a clearer articulation of risk management at the organizational level and the specific role played by senior executives. Specifically, we recommend that the framework include more material from NIST Special Publication (SP) 800-39[1], especially Chapter 2, and the Department of Energy's Cybersecurity Capability Maturity Model (C2M2)[2], specifically sections 1.1 and 5.1. Additionally, we suggest that SP-800-39 and C2M2 be included as key informative references in Appendix A for the development of an organizational risk assessment within the identify function.

Our experience informs us that engaging the organizational level is a necessary prerequisite for bridging the gap between the business environment and the development and adoption of appropriate governance structures, policies and procedures, resource allocations, awareness and training measures, and security controls for cybersecurity. Harvard Business School professors Robert Kaplan and Anette Mikes have observed that risk management is difficult and nonintuitive. It requires organizations to understand and manage different types of risk, such as preventable risks that are well handled through a rules-based compliance model to external threats that require an entirely different risk management approach[3]. Cybersecurity includes both of these types of risk and requires senior executive attention to most effectively implement a cybersecurity strategy and build the necessary resilience for a cyber event.

There are two additional benefits to ensuring an organizational-level focus for the Cybersecurity Framework. The first is that engagement with the senior-most organizational leaders on cybersecurity enhances communication between those who are responsible for the business and those who are charged with developing and implementing the cybersecurity program. The second is that engaging the organizational level helps to establish

[1] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[2] http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[3] https://hbr.org/2012/06/managing-risks-a-new-framework

organization-wide cybersecurity accountability and contributes to the development of a cybersecurity culture necessary for the most effective cybersecurity program.

Thank you for taking our views into consideration.

Sincerely,

Jonathan Litchman
Co-Founder and CEO

Dan Caprio
Co-Founder and Chairman