FIRST 72 CYBER

By Electronic Mail

February 9, 2016

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

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

I am the CEO and Founder of First72 Cyber, a Risk Management and Analytic Solutions Company focused on helping our clients better and more efficiently manage a range of cyber risks. I also previously served as the Assistant Secretary for Cybersecurity and Communications at the Department of Homeland Security from 2009-2012 and as the Chief Information Security Officer (CISO) of two publicly traded companies. In these roles, I have seen first hand the challenges that entities in both the public and private sector face when attempting to develop good metrics to identify strengths and weaknesses in cybersecurity. These challenges have historically made it difficult to develop consistent, repeatable and objective measures of cybersecurity posture that can be used by enterprises to intelligently achieve cost effective risk reduction across complex ecosystems.

We believe that the Cybersecurity Framework Core can significantly enhance the ability of Critical Infrastructure companies across the United States to improve the security and resiliency of all the systems they leverage to deliver critical services to the American public. By creating a lexicon and methodology that establishes common, discrete areas for evaluation (the Functions, Categories and Subcategories), the Framework Core lays the groundwork for something that U.S. companies have been seeking for decades—clear benchmarks that can be used by an enterprise to consistently evaluate itself and all of the vendors, suppliers, partners and advisors on which it relies.

In conversations with everyone from Corporate Boards of Directors to community groups, I often cite the maxim that in Cybersecurity, “you don’t have to be faster than the bear, you just have to be faster than the other people running away from the bear.” In the past, determining who was “faster” from a cyber security perspective (in other words, more secure) was largely anecdotal—but the Framework lays the foundation for much more granular and powerful apples-to-apples comparisons across lines of business, companies, industries-and potentially beyond—all rooted in anonymized data.

Our company and our toolset for cyber assessments was built on the foundation of the NIST Framework—by leveraging the Framework as an organizing construct, we have developed solutions that make the process of evaluating implementation of the cybersecurity standards that underpin it (e.g. ISO 27001, COBIT5 and NIST 800-53) faster, easier and more consistent. When paired with detailed subject matter expertise, our NIST Framework based tools allow companies of all types and sizes to directly evaluate and compare their internal cybersecurity risk across lines of business, operating divisions and products, and then use the same criteria to assess the cybersecurity risk associated with functions they have outsourced to vendors and partners. These solutions, or others like them, have the potential to significantly increase real understanding of the cybersecurity risks of an enterprise's entire technology ecosystem and facilitate more efficient and effective methods to reduce those risks across the nation.

In an area that is highly technical, these types of numerical ratings and benchmarks will allow Boards of Directors, internal Executive Management and line of business leads to understand where an entity is, where it's going, and how it compares to the industry--and where appropriate, other industries. While cybersecurity threats will continue to evolve, this type of approach raises the real possibility of standardizing and optimizing expenditures on cybersecurity risks—just like other risks that US companies have learned to manage over time.

Like a previous commenter, I agree that the Framework should continue to be updated and expanded over time. I would advocate very strongly that the Informative References also continue to be updated. The Framework acts as a type of Rosetta Stone for the plethora of international standards that address cybersecurity. This has significant value to anyone attempting to evaluate the cyber posture of any function that leverages systems that were built to different standards (an all too common scenario in our merger and acquisition driven economy). The ability to compare a COBIT shop with an ISO one further breaks down the artificial barriers that make cybersecurity risk management more complex than it needs to be.

Thank you for the opportunity to provide feedback via this request for information.

Respectfully,

Greg Schaffer
CEO and Founder
First72 Cyber LLC