777 Westchester Avenue, Suite 101, White Plains, NY 10604
p. 914.743.5100 | www.aponixft.com | e. info@aponixft.com

October 8, 2014

Diane Honeycutt
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: National Institute of Standards and Technology RFI
Experience with the Framework for Improving Critical Infrastructure Cybersecurity
Docket Number: 140721609-4609-01

Dear Ms. Honeycutt,

I would like to take this opportunity on behalf of the entire Aponix Financial Technologists team to thank the National Institute of Standards and Technology for your continued efforts around cybersecurity. President Obama's Executive Order 13636 brought unprecedented and necessary attention to cybersecurity. Similarly, the SEC's issuance of the April 2014 Risk Alert, which focused on technology and cybersecurity preparedness, sparked cybersecurity awareness in financial markets.

Our brief response to the NIST RFI takes a private sector view of the NIST Cyber-Security Framework, as holistic assessors of information technology risk at firms in financial markets, and advisors in cybersecurity and information technology governance. We take this opportunity to share our thoughts based on our findings of the general market, with primary data collected from our events and engagements. With regard to "*Current Awareness of the Cybersecurity Framework*", we have found that key executives of small to mid-sized financial firms are generally:

1. unaware that cybersecurity applies to them or believe they are too small to be relevant,
2. of the belief that technology vendors or internal staff handle cybersecurity for them and as a result it is not their problem,
3. convinced that cybersecurity is mostly a perimeter concern, often reduced to a firewall, and
4. uncertain of where to turn for guidance or validation outside of their internal IT staff or external IT providers.

A major industry concern we raise given these views is that these firms largely believe that they hold no responsibility in acting to mitigate cybersecurity risks. We believe that regulatory agencies should move forward in requiring firms to receive an entirely independent assessment of their technology risk, much the way firms are required to conduct financial audits. We would argue in fact that a technology assessment is more critical today than a financial audit, because corporate accounting runs on technology, as do so many other critical elements of operations.

Further, we believe the NIST framework's references to risk assessments ought to specify *independence*, as our experience has been that many information technology providers are offering risk assessments, but they are a disservice to their clients in attempting to validate their own work. An independent third-party review of the infrastructure will often find many risks overlooked by the provider, and eliminate the conflict of interest presented by self-assessment. At larger organizations, independent teams may be formed that provide third-party insights, while still employing the services of third-party assessors as appropriate.

Our opinion is that more market awareness is required to ensure that the private sector understands the real risks facing corporations today, and that they can contribute to improving our nation's threat intelligence. While Aponix continues to educate the market through events, with representatives (past and present) from agencies such as the DHS, FBI, and SEC, our reach is quite limited given such a vast audience. We greatly appreciate the investment and efforts of the NIST-related C^3 Voluntary Program in its outreach and educational efforts, and we hope to see continued funding and investment in that program.

In responding to the "*Experiences With the Cybersecurity Framework*" section of questions; most firms, particularly smaller firms, lack technology governance expertise, and their experience in implementing a technology governance framework is very limited, or non-existent. This often leaves firms hoping, without validation, that their IT and/or software providers have such expertise and experience. While these firms are often focused on service delivery and have adopted best practices of the ITIL ilk, comprehensive and adequate IT governance is not yet customary. Aponix has already found two critical governance deficiencies at two major financial services technology vendors, deficiencies that could shutdown an entire firm, at least temporarily. If a coordinated attack were executed properly, these deficiencies could cripple an entire segment of the financial services sector given the market share of these two firms. Suddenly, smaller firms in aggregate could become a systemic risk due to the lack of proper controls at their provider.

The "Roadmap for the Future of the Cybersecurity Framework" makes a key assumption that we believe is flawed.

> *"NIST intends to conduct a variety of activities to help organizations to use the Framework. For example, industry groups, associations, and non-profits can be key vehicles for strengthening awareness of the Framework. NIST will encourage these organizations to become even more actively engaged in cybersecurity issues, and to promote – and assist in the use of – the Framework as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks."*

It assumes that firms will actually care, and our experience finds that they did not until the SEC Risk Alert made them care. It frightened firms into thinking the questions asked in the OCIE's "sample list of requests" might soon be compulsory. Regrettably, despite what the SEC has intimated, some firms still believe cybersecurity is not their responsibility and are willing to address future SEC questioning as it comes.

On behalf of the entire Aponix team, thank you for the opportunity to respond to this RFI, and for NIST's continued cybersecurity initiatives.

Yours sincerely,

Marc Lotti, CGEIT, PMP
Founding Partner & COO
Aponix Financial Technologists