Weil, Gotshal & Manges LLP

767 Fifth Avenue
New York, NY 10153-0119
+1 212 310 8000 tel
+1 212 310 8007 fax

Paul A. Ferrillo

By Electronic Mail

January 11, 2016

Members of the 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 Sirs:

I am a senior counsel at the law firm of Weil Gotshal & Manges LLP in New York City, New York, and one of the leaders of its Cybersecurity, Data Privacy and Information Management practice. In general, I counsel multi-national and US-based clients and boards of directors on matters of federal securities law, corporate governance and cybersecurity law and governance at both the federal and state level. I also counsel regulated entities and advisors (like e.g. private equity funds) on their cybersecurity posture as it relates to specific guidance issued by the U.S. Securities and Exchange Commission's Office of Compliance, Inspections and Examinations. I am also a frequent commentator and writer in the area of cybersecurity.[1] By virtue of this role, I am fully familiar with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework (the "Framework") and the benefits it has already, and will continue to bestow on corporate America and perhaps the world at large at some point if adopted by other countries.[2]

It is my understanding that the NIST is look for commentary or feedback "about the variety of ways in which the Framework is being used and the relative value of different parts of the Framework, the possible need for an update of the Framework, how best practices for using the Framework are being shared and might be enhanced, and the long-term governance of Framework." It is my pleasure to give

---

[1] See e.g., "Navigating the Cybersecurity Storm: A Guide for Directors and Officers," available at http://www.advisenltd.com/navigating-cybersecurity-storm/.

[2] I addressed this organization last year on the tremendous value to Framework brings to corporate America. See http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-ferrillo.pdf.

you some preliminary feedback on our use of the Framework and how it has performed in various areas of business on a day-to-day basis.[3]

The Framework, Provides a "Common Language" to Break Communications Barriers

Coming from one highly regulated area (GAAP accounting) to the world of cybersecurity, I was initially stunned about the lack of guidance and support for how companies can and should react to the fast-changing cyber ecosystem, and how they could and should respond to cybersecurity threats aimed at their companies most critical IP and business information (e.g., personally identifiable information and credit card information). And then I read the Framework from cover to cover, and was stunned by its elegant simplicity in an area which is far from intuitive. Here is how I see the Framework best used in real-life day to day practice:

1. The Framework Core is the Rosetta Stone of Cybersecurity: In almost daily discussions with clients, I focus upon the Framework Core: Identify, Protect, Detect, Respond, and Recover. Especially the first two elements "Identify" and "Protect." If a corporation or regulated fund has not identified its important IP and informational assets and where they are located, the idea of creating a mature cybersecurity posture is no more than a fleeting proposition. Similarly, if you have not valued and assessed your most important IP and informational assets, it would be difficult to not only have a fulsome plan about how to protect them currently, but also how to better protect them in the future. Clients understand "Identify and Protect. And discussions about Identify and Protect generally lead to important discussions about other jurisdictions where data is kept (e.g., the UK or EU) which may have different cybersecurity or privacy rules and regulations, or if it is kept in a "cloud computing" environment (hereinafter referred to as "the Cloud").

2. Detecting Ransomware, Stealthware and Ghostware: Like "Identify and Protect," the "Detect" element of the core is similarly important, but for different reasons. Industries vary from sector to sector. Hardware varies from sector to sector. And with aging physical infrastructure and computer architecture, you never know what you are going to find. With the advent of more difficult to find malware, the "Detect" element forces companies and boards and IT executives to deal with fast-changing threats like stealthware, ghostware and the current epidemic of ransomware.

3. Respond and Recover = Resiliency: These elements of Framework encourage executives to think about responding to the likely fact they "have already been breached, or have been breached but just don't know it yet." Today, the recovery aspect is ever so

[3] The views I express here are my own and do not necessarily reflect the views of our clients.

important, as the ransomware epidemic has hurt not just individuals, but businesses (large and small) as well. It is thus critically important to talk about back up procedures, tapes, back up locations, and business continuity planning and testing. Paying ransomware once to cyber gangs is like open Pandora's box. Once it's open, it's hard to get it shut.

"The Need to Update the Framework"

At this point, I am not sure that the Framework needs to be "updated." My own personal view is that "**expanded**" is probably the better term of art. It is my view that the Framework should not just be limited to critical infrastructure. It would be beneficial to any company or any firm to have discussions relating to Framework's Core. Especially in the small-to-medium size business ("SMB") sector where there is also a cybersecurity threat, but where capital and sufficient standalone cybersecurity might be obtainable on a cost effective basis.[4] For example, we even use the Framework for our not-for-profit clients in order to sensitize them to the different types of information they hold (someone of which could likely be PII and thus protected under some federal or state statute or law). All business (for profit or not for profit) can benefit from use of the Framework. Whether one would call this "expansion" or "updating," the Framework should be suggested also for companies expanding products or services relating to the Internet of Things, where there likely will need to be multi-level discussions of physical devices (created in plants run by network servers) which are for instance connected to sensors and other network servers. How best to have such a discussion? Though a step by step approach using the Identify and Protect elements of the Core.

"How Best Practices Are Being Shared and Might be Enhanced"

In my view, there has been insufficient publicity on the salutary uses of the Frame to motivate and crystallize much needed cybersecurity discussion by and between companies, boards, executives and IT staffs. We know of "case by case" uses of the Framework, or we know of the Framework "by inference," but there is no method or means to communicate how or why the Framework "work" in real-life to better the cybersecurity posture of a particular company. Maybe with the passing of CISA there will be more "information-sharing" in general as it relates to cybersecurity threats, but that might not be enough to stimulate discussion around more general principles like the Framework. Might the NIST create a bulletin board approach to "wins" using the Framework? Are there other alternatives? Probably. But more people need to know that the NIST works, and works well.

I have no view of the long term governance of the Framework. In the cybersecurity ecosystem, to me "long term" means 3 to 6 months at most. But ultimately I think that is Ok. Though I had no

[4] Indeed, reference to the Framework is already contained in some regulatory documents (e.g., in the SEC OCIE "Examination Guidance").

involvement in the drafting of the Framework, I view it as a "living and breathing" document that can be referenced not matter what the threat actor, threat vector or where data is being stored (the server room, the cloud, or in some other country). And perhaps that is the Framework's best and highest use. But its benefits far, far exceed its risks, and expanded use of the Framework would not hurt a soul.

I am happy to answer whatever questions the NIST has regarding this statement.

Thank you for your time and consideration of this matter.

Respectfully yours,

Paul A. Ferrillo