Matthew McCabe
Marsh USA Inc.
1166 Avenue of the Americas
New York, NY 10036-2774
+1 212 345 9642
matthew.p.mccabe@marsh.com
www.marsh.com

Mr. Alfred Lee
Senior Policy Advisor
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230

May 3, 2013

Dear Mr. Lee:

Marsh provides these comments in response to the Notice of Inquiry (the "Notice") issued by the Department of Commerce, National Institute of Standards and Technology and the National Telecommunications and Information Administration on March 28, 2013, which solicited updated comments on the June 2011 "Green Paper," *Cybersecurity, Innovation and the Internet Economy.*

As detailed in the Notice, President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued on February 12, 2013, in part mandated that the Secretary of Commerce evaluate those steps needed to incentivize private sector adoption of the Cybersecurity Framework being developed by NIST. To carry out that directive, NIST and NTIA have sought comments to update the June 2011 report. The comments submitted by Marsh in this letter specifically address the question posed by the Notice: *How can liability structures and insurance, respectively, be used as incentives?*

Throughout its history, Marsh has provided thought leadership and innovation for clients and the insurance industry — introducing and promoting the concept and practice of client representation through brokerage, the discipline of risk management, the globalization of insurance and risk management services and many other innovative tools and service platforms. Marsh provides risk management, risk consulting, insurance broking, alternative risk financing, and insurance program management services to a wide range of businesses, government entities and professional service organizations in more than 100 countries.

Cybersecurity represents a burgeoning field of risk that demands innovative approaches to risk management. While the ability to readily store and share data across interconnected networks can create new efficiencies in sales and marketing, data access and retrieval, and vendor relations and interaction, gaining these efficiencies also carries inherent risks. These risks include theft or manipulation of sensitive or private information, such as financial or health records; computer viruses that can destroy data, damage hardware, cripple systems and disrupt business operations; and computer fraud.

Marsh concurs with the prior finding by the Department of Commerce Internet Policy Task Force, which described cyber insurance as an "effective, market-driven way of increasing cybersecurity" that reduces private sector vulnerability by encouraging widespread adoption of preventative measures, encouraging the

implementation of best practices, and limits the losses of companies that incur cyber attacks.[1] More importantly, Marsh provides its clients with cyber solutions that not only address damages and limit losses, but also provide personalized strategies for the mitigation of a variety of cyber incidents, including data breaches and network disruptions.

The growth in awareness of cyber and privacy risks has caused companies to manage their day-to-day cyber risks in the same way they do more traditional risks: through the purchase of insurance. The number of Marsh clients purchasing cyber insurance increased 33 percent in 2012 over 2011. Individually, these companies are also purchasing more of this insurance: Cyber insurance limits purchased in 2012 averaged $16.8 million across all industries, an increase of nearly 20% over 2011. Communications, media, and technology companies led all industries, both by average limits purchased — $33.4 million — and the rate of increase over 2011, which was nearly 36%.[2]

Accordingly, in developing the Cybersecurity Framework, NIST should view cyber insurance potentially as both an incentive *and* a solution. As NIST develops and the Department of Homeland Security implements the voluntary program to implement the Cyber Framework, Marsh believes that cybersecurity insurance can drive participation in the program. Cyber insurance should also be viewed as a component of the overall risk management strategy of participating entities.

Because no amount of cyber protections or information sharing will completely eliminate network intrusions, the private sector will require solutions to address that residual risk. Thus, the Framework should also consider what strategy will be used to address that residual risk. Insurance is already an accepted mechanism that enables organizations to identify risks and vulnerabilities, and which incentivizes the adoption of best practices. Today, Marsh regularly engages with clients to determine risk management and insurance solutions to address their complex risks, including detailed insurance gap analyses; network security surveys to assess vulnerability; security policy reviews and developments; network vulnerability scans; and assessments of internet connectivity vulnerability.

Similarly, once NIST finds agreement with the private sector on those metrics that should be used for the Framework, insurers can adapt the Framework to develop risk profiles of their customers, which in turn will enable those insurers to qualify companies for coverage and to price policies appropriately. Moreover, risk management metrics will often vary based on company size, data type, and other factors — and standards often are interpreted differently among industries. Cyber standards can quickly become outdated and require updates as threats and vulnerabilities change. In such a rapidly changing environment, flexible and market-based incentives are more suitable for driving innovation.

The Cyber Framework should also consider that cyber insurance frequently offers small and midsize companies that may lack resources or expertise with better opportunities to manage risk and to improve cybersecurity. Midsize and small companies increasingly seek efficiencies through third-party contractors,

---

[1] Department Of Commerce Internet Policy Task Force, Cybersecurity, Innovation and the Internet Economy (2011) at 23-24, available at http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

[2] See Benchmarking Trends: More Companies Purchasing Cyber Insurance, available at http://usa.marsh.com/NewsInsights/MarshRiskManagementResearch/ID/29870/Benchmarking-Trends-More-Companies-Purchasing-Cyber-Insurance.aspx.

MARSH

but by doing so rely on the cyber practices of those contractors. This is typified by cloud computing, through which third-party providers offer the delivery of information technology services, data storage, and/or software applications using the internet and remote servers. Although adopting the cloud increases the efficiency of a company's technology infrastructure, it comes with inherent risks, especially as companies aggregate data in large cloud providers.

A breach or disruption of a company's network can lead to loss of data and income, and additional expenses. The Framework should consider that insurers have the ability to combine coverage with pre-packaged, end-to-end service solutions where response mechanisms kick in upon notification to a carrier of a cyber attack or data breach. While these solutions apply primarily to small and midsize companies, network and service interdependencies among and between large, midsize, and small companies make this service relevant to the entire private sector. Accordingly, the Framework should consider the potential that private sector entities could outsource risk management solutions, especially for attacks associated with disruptions attributed to a failure of a third party.

Lastly, the federal government remains uniquely capable of defining the cyber insurance market by encouraging its most productive uses and recognizing its limitations. The federal government could help recognize the utility of cyber insurance by incorporating it into its own practices. To that end, the federal government could require government contractors and subcontractors to carry cyber insurance. Also, it remains unlikely that cyber insurance will cover every cyber catastrophic event. The federal government should confirm that the backstop protections of the Terrorism Risk Insurance Act (TRIA)[3] apply to catastrophic losses caused by cyber terrorism and explore whether additional federal intervention may be warranted for catastrophic losses under other circumstances.

In developing the Cyber Framework and the voluntary program, the federal government has the opportunity to develop processes that will, on a continuing basis, assess risk, establish protections, and mitigate the damage of cyber attacks. Cyber insurance presents a vehicle that has addressed all three of these roles, and has done so in a manner that uses market principles to adopt best practices. Accordingly, the Cyber Framework should promote the use of cyber insurance as a necessary risk transfer mechanism among participating private sector entities.

Thank you for the opportunity to provide comments on behalf of Marsh.

Sincerely,

Matthew McCabe
Senior Advisory Specialist
Marsh FINPRO

[3] See Terrorism Risk Insurance Act of 2002, P.L. 107-297, available at http://www.treasury.gov/resource-center/fin-mkts/Documents/hr3210.pdf.