JOSEPH P. GUNSET
General Counsel

LLOYD'S

December 13, 2013

Via Electronic Mail

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: FR Doc. 2013-25566—Public Comment on the Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

This letter is submitted on behalf of Underwriters at Lloyd's, London ("Lloyd's") in response to the National Institute of Standards and Technology's ("NIST") request for public input regarding the Preliminary Cybersecurity Framework ("Framework") which was published in the Federal Register on October 29, 2013. Lloyd's would like to thank the NIST for seeking comments on this extremely important emerging risk.

Lloyd's—The International Insurance Market

The Lloyd's market is over 325 years old and has been actively writing business in the US since around the time of the Civil War. Since that time, Lloyd's business in the US has grown significantly. Lloyd's is currently the largest writer of surplus lines insurance in the US as well as a major writer of reinsurance supporting US domestic insurance companies.

These remarks are offered on behalf of the Lloyd's market, which consists of 57 individual businesses or managing agents. In a market as large and complex as Lloyd's, not all minds will think alike. While these comments do not represent the views of any individual managing agent, they represent some of the present perspectives in the Lloyd's market.

Lloyd's is well known for its ability to underwrite risks that other insurers are unable or unwilling to cover. One of the greatest advantages of the Lloyd's market is that it has the ability to operate and innovate in new areas of risk. It should come as no surprise that one of those new areas is cyber risk.

Underwriting of Cyber Risk

It is clear that the insurance industry's current capacity to provide insurance coverage for cyber risk is insufficient to meet the anticipated size of the risk. However, the underwriting expertise of the Lloyd's market has enabled a number of our managing agents to become active in the area

LLOYD'S AMERICA, INC. The Museum Office Building 25 West 53rd Street 14th Floor New York NY 10019
www.Lloyds.com/US
Telephone +1 212 382 4060 Fax +1 212 382 4070 Email: joseph.gunset@lloyds.com

of cyber risk. The Lloyd's market understands its limitations and the amount of risk it can responsibly cover due to the developing nature of this field and the difficulty in estimating the scope of potential losses. Lloyd's offers a variety of standalone cyber insurance products; however, these products are narrowly written and tailored to the individual risk. Concerns about aggregation of events and unknown vulnerabilities limit the scope of cyber risk coverage.

It is important to note that this is a risk which is difficult to measure. When writing cyber insurance coverage, underwriters are particularly aware of the fact that the cyber risk landscape is rapidly evolving. There remains much to be learned about how to effectively mitigate cyber risk and build a more resilient cybersecurity infrastructure.

Lloyd's Supports the Framework, but Notes its Limitations

Lloyd's is supportive of the NIST's efforts to combat cyber risk via the Framework. In many ways, the emerging dialogue surrounding cyber risk helps to raise awareness and concern about what critical sectors of the US economy can do to protect themselves. Additionally, the dialogue has the potential to contribute to a better understanding of the risk posed by cyber threats and thereby to facilitate the development of more targeted and comprehensive insurance products.

In view of the unknown and changing nature of the threat posed, Lloyd's agrees with the NIST's reluctance to create rigid standards based on existing information about cyber risk. Proper management of cyber threats requires continuous and conscientious information-gathering to respond to the ever changing risk. Lloyd's continues to examine cyber risk and incorporate the steadily growing array of information about cybersecurity into its underwriting practices.

The current scarcity of information about this new and developing risk means that it would be premature to set static practice standards. Such standards at this early stage could possibly create an artificially low baseline for how organizations should cope with cyber risk and may, over time, become inadequate to address emerging risks. Notwithstanding, the Framework is an important step towards addressing cyber risk. At the same time, given the pace of change, even entities that implement the Framework will need to remain vigilant to new threats. It is important that the Framework is presented in a manner that makes this message clear.

Conclusion

The NIST's Framework serves as a good foundation upon which to build ever improving cybersecurity practices. While understanding of cyber risk is growing, it remains difficult to assess and the Lloyd's market therefore generally offers only very limited coverage. Lloyd's supports the continued development of more robust cybersecurity measures and is encouraged by the NIST's emphasis that the Framework is intended as an aid in implementing cybersecurity measures, rather than serving as a set of compulsory minimum standards. This is prudent given the quickly changing nature of technology and potentially novel cyber risks that may be faced in the future. The Framework is a positive first step towards a better cybersecurity infrastructure.

Lloyd's looks forward to continuing the dialogue as the Department of Homeland Security and the Obama Administration work to find ways to mitigate the cyber threats faced by critical infrastructure. We appreciate the opportunity to contribute this comment.

Very Truly Yours,