December 16, 2013

The Honorable Patrick Gallagher
Under Secretary of Commerce for Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Docket No.: 130909789 3789 01

Dear Mr. Gallagher:

The Office of Advocacy (Advocacy) of the U.S. Small Business Administration submits these comments to the National Institute of Standards (NIST) regarding its Preliminary Cybersecurity Framework, published on October 29, 2013 in the Federal Register.

Advocacy would like to commend NIST for its ongoing efforts to insure that small businesses are a part of the discussion on cybersecurity. Representatives from NIST have participated in several of our cybersecurity activities, and we thank you for your cooperation.

On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." This Executive Order placed primary responsibility on NIST to develop a cybersecurity framework. We have heard from our small business stakeholders, and we would like to share with you their comments and concerns regarding the preliminary cybersecurity framework. The comments fall into four areas: cost, compliance, education and enforcement.

The Office of Advocacy

Congress established Advocacy under Pub. L. 94-305 to represent the views of small entities before Federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration. The Regulatory Flexibility Act (RFA), as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA), gives small entities a voice in the Federal rulemaking process. For all rules that are expected to have a significant economic impact on a substantial number of small entities, Federal agencies are required by the RFA to assess the impact of the proposed rule on small business and to consider less burdensome alternatives.

Small Businesses Are Vulnerable to Cyber Attacks

According to one report, in the first three months of 2013 alone, there were over one billion Internet-based cyber attacks; 40 percent were against small businesses. To put that in perspective, these numbers mean that there were more than 51 cyber attacks on small businesses every second. Below are two examples where the damage to small businesses was significant:

- In 2009, Patco Construction Company of Sanford, Maine lost nearly $600,000 to hackers that likely gained access to passwords and security questions via an implanted virus.
- In May 2012, in one overnight attack, cyber thieves were able to rob $180,000 from a communications systems company called Primary Systems in St. Louis, Missouri.

These two small businesses were severely compromised and suffered significant losses. While specific data are not available, all indications point to numerous other incidents involving similarly situated small businesses.

In 2012, the Symantec Corporation conducted a cybersecurity survey of small businesses. The results of the survey revealed that 77 percent of small businesses thought their companies were safe from cyber threats. Resources are not available to determine if these two companies had cybersecurity programs, but there is still a disconnect between the reality of cybersecurity attacks on small businesses and what these businesses believe is taking place. Perhaps one reason why there may be such a large percentage who do not believe that cyber attacks are impacting their businesses is because the business owners may lack the technological resources to identify cyber attacks clearly. Moreover, this disconnect may exist because there is not a uniform definition of what constitutes a cyber attack.

The Preliminary Cybersecurity Framework Should Address Concerns That Are Specific to Small Businesses

Small businesses are the economic backbone of this nation. They make up 99.7 percent of all businesses in the United States. Small businesses provide nearly 50 percent of the private sector jobs and they represent 98 percent of U.S. firms that export goods. Based on 2009 Bureau of the Census data tabulated by the Office of Advocacy, firms with less than 500 employees had an annual average payroll of $363,000. The Census data is a clear indication that small businesses cannot economically survive cyber attacks. How then do we bridge the cybersecurity reality gap to incorporate this global threat into the business operations of small businesses? A first step may require positive responses to the four areas of small business concerns:

a. **Cost**. Small businesses usually operate on very thin margins and are very cautious and conscious of cost factors that do not directly contribute to the cost of production. Concerns with cost include the implementation cost of cybersecurity systems as well as maintenance costs and replacement costs. In this regard, one small business suggested a type of pro bono cybersecurity advisor who would help in trying to decide which system to acquire, while another small business suggested a best practice website.

b. **Compliance**. Compliance presented a unique level of discussion on several fronts. First, while this "preliminary cybersecurity framework" is designed to seek voluntary compliance,

small businesses are concerned that compliance may become mandatory. Moreover, there is a concern as to what extent the preliminary framework is taking in to consideration existing DOD cybersecurity regulations.

c. **Enforcement**. This concern was raised by some of our small retail businesses. Many of them are the victims of cyber attacks and they seem unable to get support from local law enforcement units. Thus their concern is to what extent does this preliminary framework flow down to the communities where the victims of the cyber attacks reside? They believe that without a strong enforcement component, the risk aversion model does not address the problem.

d. **Education**. There are nearly 28 million small businesses in the United States. These businesses range from businesses with no employees to businesses with 500 or more employees. Cybersecurity education must be institutionalized into the fabric of business formation. Cybersecurity must be an integral part of a company's business plan, financial plan and contingency survival plan.

Conclusion

The Office of Advocacy understands that this "preliminary cybersecurity framework" is just one of several additional steps that must be taken before a final framework is adopted. Advocacy also understands that the framework is an ever evolving document and thus there will be new opportunities to expand upon the above four areas. However, because of the seriousness of cybersecurity and because small businesses seem to be the frequent victims of cyber attacks, we believe that the education and best practice processes should not be delayed.

Advocacy looks forward to working with NIST on this issue of vital importance to small businesses. Please feel free to contact me or Assistant Chief Counsel Major L. Clark (major.clark@sba.gov, 202-205-7150) if you have any questions.

Sincerely,

Winslow Sargeant, Ph.D
Chief Counsel
Office of Advocacy

Major L. Clark, III
Assistant Chief Counsel for Procurement Policy

Cc: The Hon. Howard Shelanski, Administrator
OMB Office of Information and Regulatory Affairs