1156 15th St NW
Suite 502
Washington, DC 20005
www.sbtc.org

SBTC
Small Business Technology Council

October 27, 2017

Nathan J. Miller
National Ombudsman
Small Business Administration
409 3rd Street, S.W. Suite 7125
Washington, DC 20416

Dear Mr. Miller,

The NIST SP 800-171 and related DFARS (252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting") require that all contractors and their subs fully comply with the NIST document NLT 31 December 2017. Because these regulations impose a significant compliance burden on small business, we believe that these regulations should not be enforced against small business until the agencies have issued guidance. The SBTC asks that the SBA Ombudsman and the Fairness Board to investigate this matter and prevent agencies from fining or enforcing these regulations until the government has issued sufficient guidance for small business compliance. We are also sending a letter to the Chief Counsel for Advocacy asking them to investigate the agencies compliance with the Regulatory Flexibility Act.

While the 110 controls in the NIST 800-171 document are clear, the compliance process, and assurance that government documents are safeguarded to the greatest degree reasonably possible, is very complex and expensive to implement. The government has yet to issue any guidebook or manuals instructing businesses how to implement these regulations. Moreover, they do not to appear to comply with the Regulatory Flexibility Act, in that the Government did not develop separate, simplified regulations for small business. The NIST SP 800-171 and related DFARS are one size fits all. While a large firm may have the accountants and resources to comply with the regulation, most small businesses simply do not have the ability to comply with this regulation. The SBTC urges the Government to delay enforcement for small businesses until it has issued guidelines for compliance.

There are major concerns with some of the 110 controls. Small companies are requested to implement cyber security, and network monitoring capabilities that even the government and large companies do not have in place (e.g., recent penetration of the Equifax network, or Yahoo, Target, to name a few). Small companies are then expected to be responsible for preventing cyber penetrations. The tools for compliance are still under development, and prices for such network monitoring can be from a few dollars for a software package to tens of thousands of dollars annually for online monitoring services. And there is no assurance that any such services indeed provide greater security. There are hundreds of vendors that provide "security Information and Event Management" (SEIM) type software and prices vary all over the map.

The government should not expect hundreds of thousands of small companies (many of them with a single employee who may be a consultant to other defense contractors) to come up with their own solution. Small companies have no knowledge of "how much" a good solution costs, and how to evaluate the quality of the solution provided by the various 3rd party vendors. If a

cyber incident happens within a company, can it claim that their $100 solution package was reasonable protection? Or do they have to show that they spent $100,000 in order for the government to consider their system reasonably protected?

The fact that one company is hacked and another may not, is not necessarily because the amount of money each company spent on software security. It is often a random process. Cyber security professionals claim that there is no secured system that cannot be hacked. Hence what level of expenditures would the government consider as "reasonable" measure?

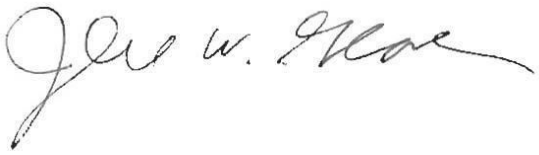
In the past year, small businesses are bombarded with offers from third party entities to help them with the compliance. The prices quoted for such services may exceed $100K. Small companies must be very careful not to fall into traps set up by such parties that do not provide any better results that the company could implement in house. Since there are no guidelines or handbook for small business, it is highly unlikely that these third parties have knowledge or information as to how the government will implement and what guidance the government will issue. Small businesses may well end up wasting time and money trying to guess how the government will enforce and what regulations and guidance that my come out.

The government should establish better guideline for what is considered reasonable safeguarding implementation, and then wait for the large contractor to implement and test such guidelines before imposing those on small businesses, factoring the cost associated with these guidelines.

The NIST SP 800-171 is a one-size-fits-all document that shifts responsibilities to the contractors, for requirements that may be impossible to assure compliance with, and doesn't take into consideration the burden it creates for small businesses that do not have the resources that larger businesses have.

SBTC asks that the SBA Ombudsman and the Regulatory Fairness Board step in to delay the agencies enforcing these regulations or fining small businesses until the government issues sufficient guidance for small business compliance.

Sincerely,



Jere W. Glover
Executive Director
Small Business Technology Council