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

November 1, 2017
Docket Number SBA-2017-0005, Reducing Regulatory Burden RFI
Topic: CyberSecurity Requirements for Small Businesses

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, relating to cybersecurity controls.

These regulations impose a significant compliance burden on small business, and the SBTC believes that the SBA should take steps to delay enforcement against small business until the agencies have issued guidance. The SBTC has also asked 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.

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. As the office of Advocacy at the SBA has pointed out in their comment to the DFARS Council, 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. In recognition of this fact, legislation has been passed in Congress to require training from Small Business Development Centers, but it will take time for small businesses to fully acclimatize to the new requirements.

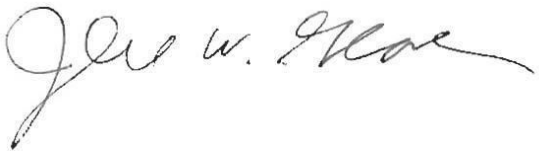
There are also major concerns with some of the 110 controls. Small companies are requested to implement cyber security, and network monitoring capabilities that even the government and large companies do not have in place (e.g., recent penetration of the Equifax network, or Yahoo, Target, to name a few). 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 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. 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, a fact this regulation doesn't take into consideration.

In the interests of reducing unnecessary regulatory burdens on small business, the SBA should step in to delay the agencies enforcing these regulations or fining small businesses until the government issues sufficient guidance for small business compliance, and gives small businesses time to adjust to the complex new rules.

Sincerely,



Jere W. Glover
Executive Director
Small Business Technology Council