Could New Cybersecurity Acquisition Plans Disrupt Federal Procurements?

Posted At : May 27, 2014 10:54 AM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Department of Defense, IT Reform, Technology Trends, Information Security, Cybersecurity, Acquisition Reform, Policy & Legislation, General Services Administration (GSA)

Growing concern over cybersecurity and vulnerabilities to cyber-attacks that would impact the supply chain of both military and civilian agencies has led the federal government to look for ways to build cyber-protections into the federal acquisition process. But some in industry are concerned that new proposals coming out of the Pentagon and GSA could be disruptive in their own right.

The joint DoD/GSA **publication**, *Improving Cybersecurity and Resilience through Acquisition - Final Report of the Department of Defense and General Services Administration*, is one component of the government-wide implementation of Executive Order 13636 and Presidential Policy Directive (PPD) 21, issued in February 2013 and both addressing improved critical infrastructure cybersecurity.

The report included six recommended reforms addressing cybersecurity and federal acquisitions:

- Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
- Include cybersecurity in acquisition training
- Develop common cybersecurity definitions for federal acquisitions
- Institute a federal acquisition cyber risk management strategy
- Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources
- Increase government accountability for cyber risk management

In the **news release** announcing the report release GSA Administrator, Dan Tangherlini noted that "the ultimate goal of the recommendations is to strengthen the federal government's cybersecurity by improving management of the people, processes, and technology affected by the Federal Acquisition System. GSA and DoD will continue to engage stakeholders to develop a repeatable process to address cyber risks in the development, acquisition, sustainment, and disposal lifecycles for all federal procurements."

Industry Concerns

The report has been open for industry comment for a few months and several IT industry organizations have expressed concerns over the direction the DoD and GSA are taking, according to **a recent account**. Specifically, some in industry are concerned that assessing cyber-risk based primarily on the inherent risk of the purchased products or services (i.e. product category) creates additional issues because it ignores the larger risk environment surrounding their implementation and it adds complexity and ambiguity that will make it difficult to use by agencies. If implemented in its current form, it sounds like it could run the risk of "the law of unintended consequences."

Implication

While the emphasis of the executive order is on using security standards to influence acquisition planning, contract administration, and to ultimately increase resiliency, agencies are also under pressure to improve the economy and efficiency of their IT acquisitions. Agencies also struggle with delays to procurements due to changing or additional requirements as well as protests. How security and resiliency controls are added to the acquisition process will have direct implications for the complexity, speed and cost of completing procurements.

Implementing good cybersecurity intentions is important, but it is equally important to implement them in the right way. Otherwise, agencies run the risk that some supply chain disruptions they experience could be self-inflicted.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@GovWinSlye**.*