Information Technology Industry Council

November 25, 2013

Defense Acquisitions Regulations System
Attn: Dustin Pitsch
OUSD (AT&L) DPAP/DARS
Room 3B855, 3060 Defense Pentagon
Washington, DC 20301-3060

Via email to dfars@osd.mil

Re: DFARS Case 2012-D050: Interim Rule on Requirements Relating to Supply Chain Risk

Dear Mr. Pitsch:

On behalf of the Information Technology Industry Council (ITI)[1], I am writing regarding DFARS Case 2012-D050, Requirements Relating to Supply Chain Security, which the Department of Defense (DoD) published in the *Federal Register* on November 18, 2013 at 78 FR 69268. By publishing this rule as an interim rule, DoD is enforcing it immediately without considering constructive public commentary. Although we appreciate the 60-day comment period on the interim rule and are preparing our comments now, we feel it is inadequate to force compliance on something as important as securing the federal information and communications technology (ICT) supply chain without first collecting the necessary input from affected parties to create an effective rule.

Lack of coordination with current efforts: By taking nearly three years to write this rule and then bypassing public consultations, DoD risks not being synchronized with the multitude of other efforts currently underway within the U.S. government on supply chain security issues, particularly those efforts that were launched after the FY 2011 NDAA was enacted.[2] Although industry might have various views on these efforts, those views have been characterized by extensive stakeholder input.

Assessment of rule's impact in question: This accelerated process also calls into question how the Department determined the rule's impact. Because DoD bypassed a public comment period, it made its own determinations, as required under Executive Orders (EO) 12806 and 13563, to "assess all costs and benefits of available regulatory alternatives and if regulation is necessary…select regulatory approaches that maximize net benefits." EO 13563 emphasizes the importance of "quantifying costs and benefits." Absent a public comment period before

[1] The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading technology companies, spanning software, hardware, and services. *See* www.itic.org.

[2] Notably, these efforts include: 1) the joint report by DoD and the General Services Administration (GSA) provided to the White House in June 2013 with recommendations on integrating cybersecurity into federal government procurement (a deliverable under EO 13866, Improving Cybersecurity in Critical Infrastructure); 2) the National Institute of Standards and Technology (NIST)'s draft Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations;" and 3) the Software & Supply Chain Assurance Forum work sponsored by the Department of Homeland Security (DHS) with input from DoD, NIST, and industry.

implementation of the rule, industry has no opportunity to provide input regarding the costs and benefits of the approach DoD has taken. DoD also conducted its own analysis under the Regulatory Flexibility Act, stating that its Initial Regulatory Flexibility Analysis (IRFA) determined that no viable alternatives exist. In essence, DoD is communicating that the matter is a *fait accompli*.

Impact on security: Among our concerns are that, as written, this rule could unintentionally but negatively impact the federal government's security, because it prevents DoD from informing suppliers about supply chain security risks the Department believes exists, and prevents any consultation with suppliers. This in turn could prevent suppliers from addressing and mitigating such risks, or lead to outdated or incorrect information being acted on by DoD. A public comment period would have allowed industry to suggest alternative approaches that could allow for risk mitigation.

Indicative of troubling trend in regulatory rulemaking process: Finally, DoD's decision to bypass public input and release a very critical procurement change as an interim rule is indicative of a troubling trend in recent years in the federal government's regulatory rulemaking process. We believe it is imperative that the public, including industry, have a voice in this process to share our expertise, experiences, and best practices with the government to produce the most effective rules and regulations. DFAR 2012-D050 exemplifies a case where the rule issued likely will have negative impacts on both innovation and security.

We urge DoD to rescind this interim rule, cease its implementation, and reissue it as a proposed rule with a robust 60-day public comment period so that all interested stakeholders can provide their input into its efficacy. We hope the Department will consider this request in a timely fashion. Please feel free to contact Erica R. McCann at emccann@itic.org with any questions or comments.

Respectfully submitted,

A.R. "Trey" Hodgkins, III, CAE
Senior Vice President
Public Sector
Information Technology Alliance for Public Sector (ITAPS)

Danielle Kriz
Director
Global Cybersecurity Policy