



January 21, 2014

Defense Acquisition 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 – Requirements Relating to Supply Chain Risk**

Dear Mr. Pitsch:

On behalf of the Information Technology Industry Council (ITI)¹ and the Information Technology Alliance for Public Sector (IT Alliance)², we appreciate the opportunity to submit comments on the interim Defense Federal Acquisition Regulation Supplement (DFARS) rule entitled "Requirements Relating to Supply Chain Risk" that was published in the *Federal Register* on November 18, 2013.³ This Interim Rule implements Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2011, as amended by Section 806 of the NDAA for FY 2013. We are concerned that, as written, the Interim Rule does not provide adequate guidance for both the DoD departments and agencies that must implement the rule and the contractors that must comply with it. Without more specific, consistent guidance, confusion and ambiguity will place stakeholders at risk of not accomplishing the statutory objectives. Moreover, given the complexity of the issue, we believe the Department must step back and ensure that an open consultative process is followed to ensure effective implementation. Below we list several

¹ The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading information and communications technology (ICT companies). ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more.

² The IT Alliance for the Public Sector (IT Alliance, ITAPS), a division of ITI, is an alliance of leading technology companies (including ICT companies and the defense industrial base (DIB)) offering the latest innovations and solutions to public sector markets. With a focus on the federal, state and local levels of government, as well as on educational institutions, the IT Alliance team advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants.

³ 78 Fed. Reg. 69268, et. seq., Nov. 18, 2013, available at <http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27311.pdf>.

1101 K Street, NW, Ste. 610
Washington, DC 20005
202.737.8888
itic.org

recommendations for changes to the Interim Rule and its proposed implementation which, we believe, will improve its effectiveness.

DFARS 2012-D050 Should Be Reissued as a *Proposed Rule*

We believe it is imperative that the public, including industry, have a voice in the rulemaking process to share expertise, experiences, and best practices with the government to produce the most effective rules and regulations. We believe that the interim rule will likely have negative impacts on both innovation and security, will increase costs for government technology acquisitions unnecessarily, will unduly burden commercial vendors, and will reduce competition through the imposition of insurmountable liabilities for contractors and their suppliers in the defense industrial base. Given this, as a threshold matter, DoD should have issued this regulation as a proposed rule. Any sense of urgency the Department is now asserting regarding this authority was lost long ago in the expired statutory deadlines and the passage of almost three years since the underlying statute was enacted. ***Industry believes that this delay is indicative of the significant challenges facing the Department in establishing a compliance regime of this complexity, and is strong evidence that the rule should be afforded a more regular promulgation process as a proposed rule*** with significant opportunities for comment by a wide range of stakeholders. The approach taken to issue the proposal as an interim final rule denies industry and other critical stakeholders with ample time, opportunity to shape, and ultimately collaborate with the Department to design a complex program that addresses multiple risks and complexities.

Estimates by DoD of the Costs and Economic Impact of this Rule are Inadequate

DoD is grossly underestimating the true costs and economic impact this rule will have on the information and communications technology (ICT) industry and defense industrial base (DIB), and the economy as a whole and has inaccurately stated those impacts in their determinations. DoD has concluded that this rule is not a “major rule” under 5 U.S.C. 804, which by definition, means that the rule will not have an economic impact of \$100 million or more on the country. Based solely on the value of current industry investments to secure supply chains and ensure product integrity, industry finds it difficult to concur with this conclusion. Additionally, the interim rule has numerous other economic impacts, including increased costs to the government customer for compliance and the additional liability costs of the provision imposed on the DIB and ICT industry. Moreover, the cumulative economic effect of the exclusion of any one company from any one contract would result in reductions in both government and commercial business, and the loss of employment at the excluded company and the corresponding loss of payroll. Other losses would be incurred as a result of the ripple effect on primes, subcontractors or suppliers to the excluded company which will lose that source of supply (and must then incur the expense of identifying and vetting new sources). Add to this the loss of income by the excluded companies and their subcontractors, suppliers and others reliant on the excluded company, the corresponding loss of tax dollars, and the loss of future business revenue from all impacted companies, it is clear the cumulative projected effects of the impacts of this rule on the U.S. economy would be well in excess of \$100 million. Thus, we respectfully disagree with and do not support the Department’s conclusion that the Interim Rule is not a “major rule” as either reasonable or accurate.

To further elaborate, industry believes that the exercise of the exclusionary authority in this interim rule and the provision to extend information about that exclusion across the Federal acquisition community will have the same effect as a permanent debarment of the company across the entire Federal government. Such a company could become known, either openly or confidentially, as a “tainted” source and their government business eventually would cease to exist. Many companies also have clauses in their commercial contracts that bar them from business if the Federal government has excluded them as a source. Should the government exclusion become known to their commercial customers, it is not unreasonable to expect that commercial business for the excluded company also would be affected, if not cease. The economic impact from the exclusion of any one reasonably sized innovative commercial company under these conditions could quickly and easily exceed \$100 million and if applied in the arbitrary and indiscriminate fashion as enabled by the interim rule, could far exceed that monetary threshold in impact across the entire industry. To further increase the total economic impact, the scope of application of the interim rule, which requires compliance at all levels of the DoD supply chain, would require significant, costly, additional investments in supplier management and compliance mechanisms by industry. We believe the scope of the application across the DIB and ICT industry, along with the substantial ongoing compliance costs would easily exceed the “major rule” threshold for monetary economic impact.

Industry is also concerned with DoD’s determination that the regulation will not have a “significant economic impact” on small business. On the contrary, the rule is likely to increase costs for smaller businesses by requiring them to significantly increase investments in compliance in order to remain at some tier in the DIB and ICT industry supply chain, by increasing liability costs associated with compliance failures, and by increasing costs associated with the heightened risk of application of the exclusionary authority and the business and economic effects noted above. In sum, the combination of increased investments necessitated by the rule, and forgone business opportunities, will likely make future DoD contracting opportunities cost-prohibitive for many small business enterprises – a fact which would amount to nothing less than a significant economic impact.

Adhering to normal order would have been the preferred, less disruptive way to implement this important rule and would have permitted a more thorough vetting of these economic impacts and their accurate valuations. ***Should the Department agree to withdraw and re-issue this rule as proposed, ITI and the IT Alliance would strongly support the convening of a public meeting prior to the re-issuance to afford further opportunity for dialogue on the impact of this rule.***

The Interim Rule Should be Integrated More Effectively into Industry and Government-led Supply Chain Risk Management Regimes in Order to Avoid Inconsistencies

The member companies represented by ITI and the IT Alliance have long shared a common interest with the Department to ensure the quality and performance of the products they manufacture or integrate for both the commercial and public sector markets. These interests have produced a multitude of industry-led initiatives to address risks that may be found in the globally sourced supply chains of today’s interconnected global economy. These industry-led efforts have also shared the objectives of scores of legislative proposals and Executive branch initiatives to better assure the Federal government

supply chain. It is more imperative than ever that these industry and government initiatives be well coordinated and transparent. Unfortunately, that is not the approach DoD is taking by injecting this interim rule into an *evolving*, government-wide supply chain risk management regime that has wide-ranging impacts on the private sector.

By taking nearly three years to write this rule and then bypassing any meaningful public consultations to better ensure alignment with other ongoing efforts, this interim requirement risks not being synchronized with the multitude of other initiatives currently underway within the U.S. government to address these issues and concerns. Although industry might have various views on these efforts, those views have been characterized by extensive stakeholder input and include the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition (i.e. the GSA-DoD 8(e) Working Group) of Executive Order 13636, the Office of the Director of National Intelligence's Intelligence Community Directive 731 and the National Institute of Standards and Technology's (NIST) draft special publication (SP) 161 on supply chain risk management (SCRM), among many others. All facets of the government have attempted to work in some fashion with industry to manage federal supply chain risks. ***It is not evident that the Department has considered how this rule fits into the current array of initiatives, or whether it would disrupt them, and thus we urge that this interim rule not be finalized until such time as it can be demonstrated that such alignment has been completed.***

This Rule Creates Significant New Barriers to the Federal Market

The interim regulation poses significant burdens for existing companies in the market, and will only further dissuade new and innovative companies from entering the public sector market. This is especially true for commercial companies who will not want to risk relationships with their commercial or international government client bases to serve the federal government. ***Any new version of this rule needs to include a prior assessment conducted with industry to determine how this significant new regulation will affect competition in the marketplace.***

The Interim Rule Should Provide Guidance to Contractors and Suppliers and Point To Relevant "Safeguards and Countermeasures"

One of the significant shortcomings industry has identified in the interim rule is that it does not provide *any* guidance about what metric will be applied to their products, services, and business models, despite referencing in the narrative on the Regulatory Flexibility Act on pg. 69269 of the *Federal Register* notice that the rule "recognize[s] the need for information technology contractors to implement appropriate safeguards and countermeasures to minimize supply chain risk." Furthermore, subparagraph (b) of DFARS 252.239-7018 requires contractors to "maintain controls in the provision of supplies and services to the Government to minimize supply chain risk." The Interim Rule, however, does not provide any guidance to contractors or government contracting officers as to the type of controls to be maintained to meet this requirement. Such ambiguity is unacceptable, as it provides no clear direction to guide investment by contractors and suppliers in the appropriate safeguards the Department is seeking from the DIB and ICT industry and does not provide the acquisition community with any guidance against which to develop the eligibility requirements and evaluation criteria necessary to implement the rule.

The inclusion of such a vague requirement almost certainly will trigger investments in practices, protocols, testing regimes, product evaluations, and personnel training, amongst others, but the lack of guidance by the Department precludes meaningful steps and investments from being made, in favor of guess work by industry. The end result of rudderless scheme contemplated by the rule will likely result in the waste of countless dollars by industry, resulting in increased costs which will ultimately be borne by DoD.

We therefore recommend that DoD issue additional guidance that uses existing and proposed global, consensus-based standards including, but not limited to ISO 27036, ISO 19770-1 on Software Asset Management and –for National Security System (NSS) procurements or other procurements for which the level of criticality warrants higher assurance—standards based on the augmentation of the Common Criteria that is being developed by industry in partnership with the National Information Assurance Partnership (NIAP) to address certain supply chain risks . By directing contracting officers to identify and contractors to follow the relevant portions of such standards, the rule will provide all sources of supply with a level playing field of understanding as to what the minimum requirements are in order to comply with DFARS 252.239-7018(b), and DoD will benefit by helping guide industry investments and by doing business with contractors that have in place the necessary minimum controls for minimizing supply chain risk. We emphasize the term “relevant” with regard to such standards so that solicitations and contracts only reference those portions of general standards that are actually applicable, and we do not create guidance that poses indiscriminate application. Any requirement that mandates “compliance” with the “standard” without identifying the specifically applicable sections only creates more ambiguity and uncertainty regarding what compliance measures are necessary.

The Interim Rule Should Provide more Guidance Regarding the Qualification Standard

The Interim Rule at DFARS 239.7305 should be amended to provide more specificity as to the type of “qualification standards” that may be established “for the purposes of reducing supply chain risk in the acquisition of covered systems.” Any established qualification standards should be required to be consistent with existing and proposed standards being used within federal agencies for supply chain risk management and could include ISO 27036, proposed NIST Special Publication 800-161, entitled “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” ISO 19770-1, and--for NSS procurements or other procurements for which the level of criticality warrants higher assurance--standards based on the augmentation of the Common Criteria that is being developed by industry in partnership with the National Information Assurance Partnership (NIAP) to address certain supply chain risks. Without such guidance, agencies’ efforts to implement successful supply chain risk management are likely to be ambiguous and inconsistent.

The Interim Rule Should Provide Guidance on Evaluation Factors

The new requirement at DFARS 215.304 for departments and agencies to consider “the need for an evaluation factor regarding supply chain risk” provides insufficient guidance as to the type of supply chain risk evaluation factors to be utilized. ***While we would expect that such risk evaluations would be conducted on a case-by-case basis, guidance should be provided as to which evaluation factors should***

be used and when. Offerors that compete for the delivery of information systems to DoD departments and agencies will better be able to prepare offers that represent the best value to the government if those contractors can reasonably anticipate how and when those controls will be evaluated with regard to contract award decisions. Again, to the extent possible, any guidance on such factors should also seek to comport with factors already being used throughout the federal government. As noted above, an array of activity is underway within the government on supply chain risk management.

It is also worth noting that a growing body of data suggests a significant correlation between an enterprise's use of counterfeit software and its susceptibility to malware and other IT security risks. Thus, any effort by DoD to reduce its exposure to cybersecurity risks should include a concerted effort to mandate within the Department the use of only legally licensed software and to eliminate counterfeit software in its own operations.

The Interim Rule Should Explicitly Require that Notice be Given to the Vendor

Congress specifically stated in Section 806 at (b)(2)(C) that the head of the agency, with the concurrence of the Undersecretary of Defense for Acquisition, Technology and Logistics (USD(ATL)) must make a determination, "in a case where the head of the covered agency plans to limit disclosure of information under subsection (a)(2)" that "the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information." It therefore stands to reason, and industry believes it was the express intent of Congress, that in all cases where such a determination is not provided under (b)(2)(C), notice *must* be given to the source so that proactive measures can be taken to mitigate or eliminate the risk determined by the Under Secretary of Defense for Intelligence (USD(I)). We also suggest the appropriate time in the process to make such a determination is the point at which the USD(I) determines a risk exists. ***Providing such a notice in advance of any procurement action would permit appropriate response to the risk. The opportunity to mitigate or eliminate the noticed risk from the supply chain would avoid significant costs that would be passed along to the Department.***

Moreover, if a determination is not made under 239.7304(b)(3), and notice is provided to the vendor, the agency should be required to offer the vendor a meaningful opportunity to rebut or remedy the allegations supporting the decision to exclude before it takes effect.

The Interim Rule Should Explicitly Require that Notice to the Vendor be Considered Prior to Exclusion

DFARS 239.7304(b)(2) of the Interim Rule requires that a decision to exercise the authority to exclude a source under DFARS 239.7305 may not be made where any less-intrusive measure is reasonably available. The underlying statute assumes that in all cases where the head of the agency has not exercised authority under DFARS 239.7304(b)(3), notice must be provided. ***We request that the proposed rule be modified to reflect the requirement for notice, and that, if a determination is made that "less intrusive measures are not reasonably available [short of exclusion] to reduce such supply chain risk," the rule should require that the notion of providing notice to the vendor has been explicitly considered and deemed unreasonable before a decision to exclude has been finalized.***

A Periodic Review of Excluded Contractors Should be Required for Ongoing Contracts with New Task Orders

As currently drafted in DFARS 239.7304(c), the agency would have no obligation to consider circumstances that might weigh in favor of removing or overcoming a barrier to competition during the pendency of an existing contract—only before a subsequent procurement is initiated. Industry believes it was the intent of Congress to treat any decision to exclude a vendor without notification as extraordinary. As such, if a vendor has been excluded without notice, the Interim Rule should require the agency to review that decision on no less than an annual basis for as long as the contract is in place. Once a decision to exclude a vendor without notice has been made, there should be some obligation to revisit that decision periodically. Over time, the equities may shift such that the costs and risks associated with not notifying the source eventually outweigh giving the source information that could be used to remedy the problem, the company may independently identify the risk and mitigate or remove it, or perhaps the problem resolves itself. ***The language should be changed accordingly to require that determinations to exclude without notice are periodically revisited and that sources of products are provided a means of becoming eligible for future solicitations.***

The Scope of the Rule is Overly Broad and Should be Narrowed to Only NSS Solicitations

The interim rule as proposed is overly broad and does not reflect the stated intent of Congress to carefully and narrowly expand existing authority to exclude sources for *national security reasons* by adding the extraordinary ability to exclude without informing the vendor and/or the prime of the reasons for the decision to exclude. Instead, DoD has side-stepped the narrow scope of the statute by applying the clause in a blanket and indiscriminate fashion to every solicitation and contract for information technology, including all contracts for commercial items, and it has avoided its responsibility as intended in the statute to take appropriate steps to mitigate and eliminate supply chain risk before the use of the exclusionary authority can be even considered, much less exercised.

To apply this rule consistent with Congress' intent, DoD should only include this implementing clauses in solicitations and contracts for specific information technology goods and services in NSS, rather than "in all solicitations for contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply" as demanded by DFARS 212.301. Since there is clear guidance established by the National Security community as to what constitutes a NSS and when such designations should be made, application of this authority to those contracts would not be difficult, and far superior to the broad approach proposed by the Department. Furthermore, the definition of "covered system" in DFARS 239.7302 is quite broad and the definition of "information technology" is defined even more expansively than in FAR 2.1, covering information systems ranging from systems used for intelligence activities to information systems used for the "direct fulfillment of military or intelligence missions." Ultimately, the successful management of supply chain risk requires the education of all members of the federal acquisition team as to when and how to meaningfully apply the new requirements of the rule, and the overly broad definitions and scope as written fail in that regard because they do not adequately or clearly identify when this rule is relevant. Without more guidance, it

is very likely that different acquisition team members will reach different conclusions for similar systems and needs.

Finally, the application of this regulation to all acquisitions of commercial items is a direct overreach by the Department and conflicts with the apparent statutory scope. Commercial companies produce their products for a global consumer base and normally would not know the identity of any final user or the application of use for any product. As such, it is not possible for a commercial company to know, in advance, of the selection of their product for use in a NSS or even that it would be sold into the supply chain for DoD. Indeed, such broad usage will cause needless confusion and increase costs because bidders will not have a clear picture of the actual requirements of a particular request for information or requests for proposal. The procurement action at issue may or may not be a *covered* one. ***The rule should be modified to reflect Congressional intent by applying the exclusion clause only in covered procurements and by providing potential offerors sufficient notice that the goods or services they offer are to be used in a covered procurement.***

Means of Remedy Should be Afforded Primes Whose Subs Are Excluded

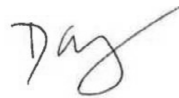
At DFARS 239.7305(c), DoD inserts itself into the prime and subcontractor relationship by authorizing the withholding of consent “for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source.” Unfortunately, the proposal does not establish reasonable remedies or relief for primes when this clause is exercised. A prime may have already established supplier relationships as part of a bid or be well into the performance period on a contract before this authority is used by the Department. Such a disruption to competitive activity or performance and sourcing of needed supplies can cause significant additional expense, violate supplier contracts, and trigger legal actions, among other risks. ***The regulation should specifically afford remedies, including equitable adjustments, whenever the authority at 7305(c) is exercised and a prime must exclude a subcontractor.***

ITI and the IT Alliance appreciate this opportunity to share our perspectives and comment on the interim rule. Should you have any questions regarding these comments, please feel free to contact Erica McCann at emccann@itic.org or 202-524-4394.

Respectfully Submitted,



A.R. “Trey” Hodgkins, III, CAE
Senior Vice President
Public Sector
Information Technology Alliance for Public Sector
(IT Alliance)



Danielle Kriz
Director
Global Cybersecurity Policy
Information Technology Industry Council (ITI)



1101 K Street, NW, Ste. 610
Washington, DC 20005
202.737.8888
www.itic.org