

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
703-875-8059

January 13, 2014

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

Ref: **DFARS Case 2012-D050 – Requirements Relating to Supply Chain Risk**
CODSIA Case 09-13

Dear Mr. Pitsch:

On behalf of the Council of Defense and Space Industry Associations (CODSIA),¹ we are pleased 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, 2013.² This Interim Rule implements Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2011,³ as amended by the NDAA for FY 2013.⁴

Our member associations have long supported congressional, departmental and industry efforts to secure the industrial supply chain. CODSIA looks forward to continuing such efforts by collaborating with the Department of Defense (DoD) to achieve the necessary solutions. We also realize and appreciate that DoD is acting in accordance with statutory language. Within the constraints of Section 806, DoD can and should take several steps to make this Interim Rule more effective and efficient.

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

¹ CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of six associations – the Aerospace Industries Association (AIA), the American Council of Engineering Companies (ACEC), the National Defense Industrial Association (NDIA), the Professional Services Council (PSC), TechAmerica, and the Chamber of Commerce of the United States. CODSIA’s member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members’ positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

² 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>.

³ Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. 111-383 (hereinafter “NDAA FY2011”).

⁴ National Defense Authorization Act for Fiscal Year 2013, Pub. L. 112-239.

As a threshold matter, DoD should have issued this regulation as a **proposed** rule. First, the new rule authorizes the exclusion of businesses from the defense industrial base, an act with the potential for putting a vendor out of business resulting from the stigma of being labeled a supply chain risk. Such authority should not be exercised without first hearing the views of and gathering all relevant information from the parties that will be directly impacted by this rule. This interim rulemaking leaves unanswered many fundamental questions about invoking the authority. The process for exclusion is unaddressed. The clauses posited for adoption contain no direction to offerors on how to proceed in the face of an exclusion, except that all offerors are under notice that they could be excluded, but may not get a debriefing nor be able to submit a bid protest to the GAO or elsewhere to determine why. The fear articulated by industry during the initial formulation of Section 806 was that a lack of notice was only one concern about a supply chain exclusion process that could lead to the “blacklisting” of a company from all federal acquisition.

Second, as Congress passed the underlying statutory authority nearly three years ago, the time DoD took to craft this rule illustrates the numerous implementation and compliance difficulties associated with the rule. In addition, DoD is adding this interim rule into an *evolving* supply chain risk management regime. DoD, the White House, NIST, DHS, and Congress are all working with industry and independently to manage supply chain risks and strengthen cybersecurity. We urge DoD to consider whether this rule fits into that process. Adhering to advance notice and public comment procedures would have been the better, less disruptive way to implement this important rule. We urge DoD to withdraw the rule and reissue it as a proposed rule to allow for a robust industry dialogue to better understand its impact and, ultimately, improve the final rule.

The Final Rule Should Reinforce Its Goal to Encourage Vendors to Better Manage Supply Chain Risk

DoD declares, “The objective of this rule is to protect DoD against risks arising out of the supply chain.”⁵ Government and prime contractor acquisition activities and program managers benefit from language that encourages additional measures for systems and component parts to reduce supply chain risk while proceeding with all other procurements not rising to the level of national security systems (“NSS”). The Final Rule should include language that reinforces the top level objective stated in the definition of supply chain risk: “This rule, by itself, does not require contractors to deploy *additional supply chain risk protections*, but leaves it up to individual contractors to take the steps necessary...to protect their supply chain.”⁶

The Scope of the Rule Exceeds the Intent of Congress and is Too Broad

The rule should be narrowly scoped to reflect the intent of Congress, which sought to give DoD the extraordinary ability to exclude sources only to protect NSS. DoD ignores the scalpel-approach taken by Congress in two ways: 1) mundane systems will be over-classified by Program Managers as NSS and 2) the rule’s provisions and clause must be included in **every** information technology solicitation and contract.

⁵ 78 Fed. Reg. at 69269 column 2.

⁶ *Id.*

NSS Classifications Should Be Reserved to an Appropriate Level above Program Manager

Currently, under DoD policy, the decision to designate/classify a system as NSS is made at a relatively low level in DoD.⁷ Though guided by NIST Special Publication 800-59, the Program Manager may have a propensity to “over” classify and subject more systems to this rule than would reasonably benefit from the extraordinary powers conferred to DoD for NSS. For example, the Navy’s platform information system, NMCI/NGEN, was classified as NSS, although it provides underlying enterprise infrastructure and is not a weapons system or command/control.⁸ By classifying larger, more mundane systems as NSS, the DoD not only increases the cost of the project, but increases the likelihood that **no** vendor would be able to complete the project because suppliers farther removed from the prime will be excluded.

DoD Should Take Steps to Clearly Designate Systems as “NSS” and Limit the NSS Classification to Only Those Systems that should be Classified as “NSS”

To further guard against over-classification, DoD should set clearer standards for designating a system as NSS, consider evaluating the classification decision and articulate to Congress, bidders and vendors when a system is NSS. DoD should have to articulate its reasons for classifying a system as NSS and include that classification in notice to the public (industry), as appropriate, in the pre-solicitation synopsis and/or in the model form contract documents. Over-classification of systems as NSS has the potential to lead to over-classification of lower-level components that prime contractors subcontract to sub-tier suppliers. Such over-classification may create a significant expense without significant benefit, and a pre-solicitation notice could help companies decide where to best direct their proposal efforts.

DoD Should Include the Rule’s Provisions and Clauses in NSS Solicitations and Contracts Only

DoD should only include this rule’s provisions and clauses in solicitations and contracts for information technology NSS rather than all information technology solicitations and contracts, i.e., only in “covered procurements.” Again, Congress authorized extraordinary powers to be used by the highest-ranking officials at DoD. As written, the rule applies far more broadly, because its provisions and clauses will be included in all “solicitations and contracts” for information technology, “including contracts for commercial items or commercial off-the-shelf items involving the development or delivery of any information technology, whether acquired as a service or as a supply.”⁹ Indeed, “information technology” is defined even more expansively than in FAR 2.1. 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 RFI or RFP, because they will only know the procurement action at issue **may or may not** be a *covered* one. Therefore, it is likely bidders will price their bid at the “covered procurement” requirement, which will likely be higher than for a non-covered procurement. DoD should 1) only insert

⁷ See DODI 50000.02 Enclosure 1 at pp.72 and 132; SECNAVINST 5000.02 at pp. 1-20 to 1-21 and 2-8 (the Program Manager is authorized to decide upon and approve decisions to classify an information system as Mission-Critical/Essential, NSS, etc.)

⁸ Capt. Timothy Holland, Program Manager, “NGEN Acquisition Industry Day Brief” (July 8, 2010) available at <http://www.public.navy.mil/spawar/PEOEIS/NEN/NGEN/Documents/NGEN%20Acq%20Industry%20Day%20Brief%20Final.pdf>

⁹ 78 Fed. Reg. at 69268 column 3.

the exclusion provisions into covered procurements and 2) provide bidders sufficient notice that they are bidders or contracting for a covered procurement. Along these lines, DoD should clarify whether the interim rules apply to cloud computing acquisitions or whether they are covered procurement actions as a class, since it is not directly addressed in the interim rules.

By Improving Due Process, DoD Can Better Secure the Supply Chain

There is a critical gap between the policy to exclude and the notice and substantive clause provisions in the interim rulemaking. While the exclusion process within DoD appears detailed and sufficiently scaled to require that proper determinations are drafted at the highest levels of DoD, the department must do more to guarantee due process to their suppliers under this rule. In DFARS 239.7305(d), DoD can limit the disclosure of information relating to the basis for carrying out exclusion actions under DFARS 239.7305(a)-(c). However, DoD should encourage notice to suppliers, to the greatest extent possible, because it will enable remediation and overall improvement in the supply chain. By only describing how to limit disclosure and ensure confidentiality, DoD here is implicitly discouraging information-sharing, even though information-sharing is being encouraged and shown to be effective in other quarters and initiatives. Moreover, because exclusions will become public, government exclusion from a competition would be tantamount to a de facto debarment without any due process for the affected firm. Indeed, the cascading blacklist effect associated with the government's direction to a contracting officer or contractor to avoid a source of supply without prior notice to the affected firm may lead to the failure of the company as a result of the stigma of supply chain risk associated with such an exclusion.

Under those conditions, despite the clause prescription of limited application only to NSS, it is fundamentally unclear that an exclusion will be made on a case-by-case basis or be a blanket exclusion of a contractor or subcontractor. Consequently, it is also unclear in the rule whether a single exclusion determination could or should apply to the three enumerated types of exclusion criteria set forth in 239.7305. Is a separate determination needed to exclude a prime contractor? Is a separate determination needed for consent to exclude that same company as a subcontractor, even though it is reasonable to conclude that exclusion will be of a specific source and thus be immaterial what stage or by what criteria a source is excluded?

For that matter, it is unclear at what point in the acquisition process such exclusions may be authorized or executed. Under the new rule's language, a source could be excluded before, during and (or) after a contract award (whether as prime or subcontractor). For most commercial IT providers, exclusion will affect their federal transactions at every step along the process. Exclusion will lead to entanglements on many fronts, on many transactions, with many differently placed customers at the same time.

Conversely, the policy at 239.7305(d)(2) is ambiguous on what parties are eligible to receive the notice of an exclusion of a company. The rule requires notice by the authorized individual to "appropriate parties" to the extent needed to execute a covered procurement action, and to DoD and other federal agencies, but makes no provision to provide notice to other federal contractors that might be impacted by the exclusion, although not related to the specific covered procurement action and that might have other contracts with the excluded party.

Notice, dialogue, and resolution, i.e. due process, serve to identify root causes of supply chain risk and allow suppliers to clear their name when falsely accused. For example, DoD may buy a piece of compromised equipment from an unauthorized reseller, such that the “supplier” should be excluded under the new 239.7305. Even though the unauthorized reseller is at fault, DoD may ban the original manufacturer without disclosing the underlying cause for the exclusion. In this case, both DoD and the manufacturer would be damaged via a lack of notice. With dialogue and due process, DoD would discover that the equipment was supplied by an unauthorized reseller, work with the manufacturer to procure a legitimate product, and spare the innocent manufacturer reputational and direct exclusionary damage. Due process preserves the trust on both sides of contracts, especially in long-term projects. In sum, it is a terrible contradiction to foist all responsibility on vendors who do not and cannot know the reasons underlying a specific exclusion action by DoD. An elaborate internal process is no substitute for a robust, clear, and certain external process.

By Focusing on Remediation, DoD Can Better Secure the Supply Chain

While DFARS 239.7305 allows DoD to exclude sources, it—or any other new DFARS clause—does not provide a pathway to reinstatement or inclusion once a supplier is excluded. Once DoD wields its scalpel, a vendor should be allowed to demonstrate supply chain risk is under control and rejoin the defense industrial base. The goal of the underlying legislation was to reduce risk and protect the supply chain; exclusion is simply a means to achieve that goal. If vendors can successfully demonstrate they meet the criteria for supply chain risk management and mitigation, then they should be welcomed back into the defense industrial base. With the lack of notice or a clear due process as described above, a pathway back for responsible vendors is all the more important. DoD should provide criteria for demonstrating adequate remediation. Since the scope of this rule does not contemplate specific steps to reinstate companies after an authorized exclusion—and there is no evidence in place to understand the impact of this rule over the near term—we propose that DoD establish a separate rulemaking as soon as practicable and coordinate a unified policy with an industry-government working group to gain insight into how remediation and rejoining the defense industrial base can be accomplished in a responsible manner.

DoD Should Provide Equitable Adjustments and Other Remedies for Primes Whose Subs Are Excluded

Under DFARS 239.7305(c), DoD may withhold consent for a contractor to subcontract with a particular source or direct a contractor to exclude a source. The new regulations fail to provide relief for prime contractors who must exclude a source through no fault of the prime. For example, the source in question may be excluded based on an unrelated project. Yet, the contractor may already have put together its bid or started work. DoD should provide equitable adjustments and other remedies to compensate contractors who must expend unanticipated resources to find a new subcontractor, who find it commercially impracticable to perform once a source is excluded, or who are liable for unjust exclusion because the sub was not told why it was excluded by the prime due to confidentiality requirements. In addition, DoD should provide equitable adjustments for any retroactive application of this rule.

Excluding a supplier can make it impracticable, if not impossible, for a prime contractor to perform a contract. On any program, a given subcontractor may be the only source available to the prime contractor. Even if other sources are theoretically available, requalifying an additional source can take a very long time and be extremely costly. On an existing program, a prime contractor may be unable to proceed with performance until a substitute subcontractor is located. In addition to the time and cost of requalification (assuming another source can be found), there are likely to be very significant costs associated with delays in performance, redesign costs and other adverse impacts on the program.

The fact that the clause is written to require flow-down to subcontractors regardless of tier suggests the government intends to have the right to direct a supplier at any tier to be excluded for a contract. This could lead to even greater disruption of a program supply chain since the loss of a supplier at a remote tier can have ripple effects on all higher-tier contractors. The potential costs for the delay, disruption and workarounds required to address the situation could be enormous.

Failing to address the effects of exclusion of subcontractors almost guarantees that implementation of this rule will result in claims and disputes, and almost certainly litigation that will prove to be expensive and difficult to resolve.

This Rule Creates Numerous Implementation Challenges

The new DFARS 252.239-7018 (b) declares, “The Contractor shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk.” Earlier, DoD claims in the Regulatory Flexibility Act explanation that:

This rule, by itself, does not require contractors to deploy additional supply chain risk protections, but leaves it up to the individual contractors to take the steps they think are necessary to maintain existing or otherwise required safeguards and countermeasures as necessary for their own particular industrial methods to protect their supply chain.¹⁰

While we do not suggest DoD explicitly endorse one set of controls over another, industry does need some guidance beyond “maintain controls.” Industry and government are working hard to develop standards and best practices. It is not clear what controls (if any) DoD expects of contractors other than adherence to and flow down of the IT excluded parties’ restrictions. This regulation seems to create a parallel DoD excluded parties list, but only applies to providers of IT. The definition of covered items appears to include products involving command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions. It is not clear how DoD will publicize this list. Perhaps the entities excluded by DoD for IT supply chain risk would be identified on the existing excluded parties list website.

In addition to the costs described above, this rule creates uncertainty by failing to describe how supply chain risk will be used as an evaluation factor (DFARS 239.7301(a)). When managing risk, the

¹⁰ 78 Fed. Reg. at 69269 column 2-3.

government must realize that the steps necessary to exhaustively test all software to eliminate all potential unwanted functions is unaffordable.

Regarding new DFARS 239.7305, "Exclusion and limitation on disclosure," will the government identify examples of the "qualification standards" and "acceptable rating" that sources must meet? Are these NIST, DoD or international standards? The rules reference a failure to meet a qualification standards in 10 U.S.C. 2319 as one way to determine how to accomplish, facilitate, or suggest a source exclusion. However, the statute at issue was created to encourage competition by establishing threshold levels for testing processes or quality assurance that could be used as predicate requirements for participation in any given acquisition by putative offerors. DoD gives no indication in this rulemaking for creating a framework for qualification processes or one commonly applied standard to evaluate IT systems supply chain risk. At present, it is reasonable to conclude that most IT contractors and vendors would not meet any 10 U.S.C. 2319 requirements, absent a huge DoD effort to address that gap between the statute and this rule.

There must be consistency in the call out of the relevant Supply Chain Risk Management (SCRM) standards and ratings in RFPs because it will create an unnecessary administrative burden for contractors to select its suppliers and subcontractors based on a moving target of standards and ratings. Furthermore, if there is not a minimum standard called out, then a contractor could become "uncompetitive" in source selection by imposing stricter standards upon its suppliers and subcontractors than other bidders. If more than the bare minimum is desired, then source selection evaluation factors should provide "win points" for SCRM in a proposal. Currently, bidders can only "lose" a competition (pass/fail) by a weak response in SCRM and Information Assurance. There is no incentive to do better than the minimum.

There is a significant difference between a statutory authority to exclude based on a determination executed at the highest levels of the DoD acquisition and Intelligence infrastructures and the application of a rating of less than "acceptable" in a source selection process conducted by a rank and file contracting officer. If a company receives a less than "acceptable" rating in a source selection, how is that rating completely determinative of their holistic supply chain risk to their customers in the sense contemplated in this rulemaking? It is not far-fetched that the term "acceptable" in a source selection means different things to different contracting officers and could thus have serious unintended consequences to companies exposed to that authority, whether it is as prime or subcontractor. Is a company that receives a less than "acceptable" rating in any given transaction required to then be proposed for an exclusion determination by a contracting officer? The exclusion process is seriously flawed because it does not connect the acts conducted by those at higher levels in DoD with the actions of the contracting officers in any rational time phased application that would help federal sellers understand the proposal and business risk involved in any given source selection process.

We also request DoD clarify the definition of "Supply Chain Risk." DoD should clarify the phrase, "maliciously introduce unwanted function," clearly explaining if this is a hardware or software concern or both, and recognize that threats posed "maliciously" are just one class of threat. Similarly, DoD should clarify whether or not the rule applies to embedded processing. The original language of DTM 09-

016 tied major weapons to embedded processing explicitly. While weaving this rule into the many supply chain and cybersecurity risk reduction initiatives presently underway, DoD should take great care to not create a situation where this rule will be waived because it is unrealistic (e.g., Information Assurance certification requirements) .

The requirements of Section 806 expire on September 30, 2018.¹¹ We recommend that DoD catalog the number of source exclusions executed under this authority that occur between 2013 and 2018 and, pursuant to any further information or a significant change in operative conditions, allow the authority to sunset as scheduled unless there is evidence that it is still needed to protect against supply chain risk.

DoD Should Close Implementation Loopholes Created by the Supplementary Information

The Supplementary Information in the Federal Register publication of the DFARS Case 2012-D050 appears to create significant contractor discretion in the rule implementation. Section IV “Regulatory Flexibility Act” text regarding the implementation of the rule states:

This rule does not require any specific reporting, recordkeeping or compliance requirements. It does, however, recognize the need for information technology contractors to implement appropriate safeguards and countermeasures to minimize supply chain risk. This rule, by itself, does not require contractors to deploy additional supply chain risk protections, but **leaves it up to the individual contractors to take the steps they think are necessary to maintain existing or otherwise required safeguards and countermeasures as necessary** for their own particular industrial methods to protect their supply chain. (Emphasis added.)

While this language is not evident in the “rule” text itself, its placement in the Supplementary Information creates a condition where some competitors will race to do the “least” to win in a “low bid, minimum acceptable” environment.

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 defense space and civil space. This is especially true for commercial companies who will not want to risk relationships with their commercial client base to serve the federal government, or for their international government clients to retaliate.

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

Our numerous concerns over scope, due process, remediation, and implementation all indicate that this rule may very likely be have over a \$100 million economic impact and, therefore, should be considered a “major rule” under 5 U.S.C. § 804.¹² While the department is correct that “companies have an existing interest in having a supply chain that it can rely on to provide it with material and supplies that allow the contractor to ultimately supply its customers with products that are safe and that do not impose threats

¹¹ National Defense Authorization Act for Fiscal Year 2013, Pub. L. 112–239.

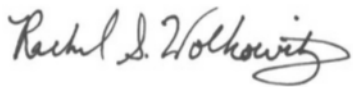
¹² We sincerely hope DoD will address our concerns, allowing the Department and public to have an accurate picture of the rule’s economic impact.

or risks to government information systems,” this rule creates costs beyond the supply chain risk management a responsible company would undertake in the course of ordinary business. For example, given the effect of exclusion on any single impacted company, the rule could easily have an impact exceeding the \$100 million threshold. Further, 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 industrial base, along with the substantial ongoing compliance costs would easily exceed the “major rule” threshold for monetary economic impact. While this does not change the ability of DoD to issue a rule as interim in the case of “urgent and compelling reasons,” it does increase the level of justification and due diligence the department must undertake to promulgate this rule and it is discouraging to the stakeholder community that DoD has understated the cost associated with this regulation.

Conclusion

Thank you for your attention to these comments. We welcome the opportunity to meet to discuss these comments. In the interim, if you have any questions or need any additional information, please do not hesitate to contact Rachel Wolkowitz of TechAmerica, who serves as our project officer for this case, or Bettie McCarthy, CODSIA’s administrative officer. Rachel can be reached at (202) 682-4442 or at rachel.wolkowitz@techamerica.org. Bettie can be reached at (703) 875-8059 or at codsia@pscouncil.org.

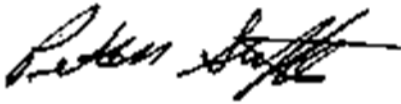
Sincerely,



Rachel Wolkowitz
Assistant General Counsel
TechAmerica



Christian Marrone
Vice President, National Security & Acquisition Policy
Aerospace Industries Association



Peter Steffes
Vice President Government Policy
National Defense Industrial Association



R. Bruce Josten
Executive Vice President, Government Affairs
Chamber of Commerce of the U.S.



Mark Steiner
Senior Director, Federal/International
Programs
American Council of Engineering Companies



Alan Chvotkin
Executive Vice President & Counsel
Professional Services Council