U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF ADVOCACY
REGULATION • RESEARCH • OUTREACH

February 29, 2016

VIA ELECTRONIC SUBMISSION

Mr. Dustin Pitsch
OUSD(AT&L)DPAP/DARS
Room 3B941
3060 Defense Pentagon
Washington, DC 20301-3060

Re: Interim Rule, Defense Federal Acquisition Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), 80 Fed. Reg. 51739 (August 26, 2015), amended in 80 Fed. Reg. 81472 (December 30, 2015)

Dear Mr. Pitsch:

The U.S. Small Business Administration's Office of Advocacy (Advocacy) submits the following comments in response to the Department of Defense's interim final rule, "Defense Federal Acquisition Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)."[1] Advocacy believes DOD has underestimated the substantial number of small businesses affected by this rulemaking and the significant economic impact of compliance. Advocacy recommends that DOD include small businesses serving as prime contractors and as subcontractors in their estimation of the number of impacted small entities. Advocacy also recommends that DOD consider alternatives, such as collaborating with universities or other organizations to provide low-cost cybersecurity services to small businesses, or providing a one-time subsidy to small businesses to help cover the cost of initial consultations with third-party vendors.

The Office of Advocacy

Congress established Advocacy under Pub. L. 94-305 to represent the views of small entities before Federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration. The Regulatory Flexibility Act (RFA),[2] as

[1] 80 Fed. Reg. 81472 (December 30, 2015).
[2] 5 U.S.C. §601 et seq.

amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA),[3] gives small entities a voice in the rulemaking process. For all rules that are expected to have a significant economic impact on a substantial number of small entities, federal agencies are required by the RFA to assess the impact of the proposed rule on small entities and to consider less burdensome alternatives.

The Small Business Jobs Act of 2010 requires agencies to give every appropriate consideration to comments provided by Advocacy.[4] The agency must include, in any explanation or discussion accompanying the final rule's publication in the Federal Register, the agency's response to these written comments submitted by Advocacy on the proposed rule, unless the agency certifies that the public interest is not served by doing so.[5]

Background

On August 26, 2015, the Department of Defense (DOD) published an interim final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement security requirements specified by a National Institute of Standards and Technology Special Publication, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (NIST SP 800-171). On December 30, 2015, DOD published an interim final rule[6] in the *Federal Register* that provided large and small contractors with more time to bring their companies into compliance with the August 26th rule.[7] The requirements in SP 800-171 are designed for use in protecting sensitive information residing in contractor information systems. Under the December 30 rule, all contractors' systems must be compliant with NIST SP 800-171 security requirements no later than December 31, 2017. However, the December 30th rule still currently requires contractors, within 30 days of contract award, to notify DOD of any NIST SP 800-171 security requirements that are not implemented at the time of contract award. Thus, even with the additional time for businesses to become fully compliant with the interim regulation, new contract awards will require contractors to record their progress toward full compliance with NIST SP 800-171. This interim rule requirement appears to be an attempt to ensure that DOD is provided with accurate reports identifying gaps each time contract performance begins under a new award. However, contractors will not be allowed to have security system gaps when full compliance starts on December 31, 2017.

NIST 800-171 establishes a set of procedures for "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." NIST SP 800-171 focuses on minimum standards and best practices with 14 "Security Requirement Families" and provides a detailed list of basic and derived security requirements contractors need to implement to meet each of the standards. The 14 requirements are:

1. Access control
2. Awareness and training

---

[3] Pub. L. 104-121, Title II, 110 Stat. 857 (1996) (codified in various sections of 5 U.S.C. §601 et seq.).
[4] Small Business Jobs Act of 2010 (PL. 111-240) §1601.
[5] *Id.*
[6] 80 Fed. Reg. 81472 (December 30, 2015).
[7] 80 Fed. Reg. 51739 (August 26, 2015).

3. Audit and accountability
4. Configuration management
5. Identification and authentication
6. Incidence response
7. Maintenance
8. Media protection
9. Personnel security
10. Physical protection
11. Risk assessment
12. Security assessment
13. System and communications protection
14. System and information Integrity

Advocacy has been engaged with small businesses, industry representatives, and the Federal government on cybersecurity for several years. Advocacy has worked with NIST, GSA, DOD and DHS on multiple cybersecurity acquisition requirements issues and their impact on small businesses.

Advocacy's comments on the DFARS Interim rule

Advocacy would first like to commend the DFAR team for listening to industry and agreeing to delay the full implementation of this cybersecurity rule until December 31, 2017. Advocacy is also appreciative that the DFARS Council has requested comments from the industry and from small businesses on the DOD implementation strategy of the compliance requirements for NIST SP 800-171.

Advocacy has two chief concerns with the December 30 interim final rule. First, DOD's initial regulatory flexibility analysis (IRFA) appears to be deficient in its estimation of affected small businesses and does not to consider significant alternatives. Second, the cost of compliance with the rule will be a significant barrier to small businesses engaging in the federal acquisition process.

A. DOD's IRFA appears to be deficient.

Number of Small Entities. Advocacy believes that DOD's estimation of the number of small businesses affected by the rule is too low. DOD should include both small business prime contractors and small business subcontractors when estimating the number of small businesses impacted by the interim regulation. This rule will apply to all contractors with covered defense information transitioning their information systems. DOD estimates that 10,000 contractors will be impacted by this rule and no more than 5,000 will be small businesses.[8] It is unclear from DOD's analysis whether this estimation includes prime contractors, subcontractors, or both. As discussed below, DOD's interim rule will significantly impact small businesses serving as prime contractors as well as small businesses servings as subcontractors. If DOD's estimation only includes small business prime contractors, Advocacy believes DOD has vastly underestimated the number of small businesses affected by this interim rule.

[8] 80 Fed. Reg. 81472 (December 30, 2015).

Significant Alternatives. In the December 30 rule, as in the August 26 rule, DOD asserts that "[n]o significant alternatives, that would minimize the economic impact of the rule on small entities, were determined."[9] However, the Regulatory Flexibility Act (RFA) requires discussion of such alternatives as:

> "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities;
> (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for small entities;
> (3) the use of performance rather than design standards; and
> (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[10]

Consistent with the requirements under the RFA and to help alleviate the economic burden the interim final rule will place on small businesses handling covered information, Advocacy recommends that the Federal government consider either:

- Collaborating with universities and other organizations to provide low-cost cybersecurity services to small businesses participating in the federal acquisition process. These institutions would provide services to supplant contracts with third-party vendors for assessments of information systems and security controls and for cybersecurity trainings and manuals for their employees;

- Providing a one-time subsidy to small businesses participating in the federal acquisition process to help cover the cost of initial consultations with third-party vendors to assess their information systems and security controls for vulnerabilities. This one-time subsidy would be provided to these small businesses when they initially enter the federal acquisition process; or

- Other significant alternatives as described by interested parties.

Advocacy suggests that DOD provide the public with its analysis on each of these alternatives. Given that DOD determined the entire industry, both large and small businesses, needed additional time to comply with the August 26 rule,[11] DOD should at least consider a further extension of the compliance time for affected small businesses.

B. The cost of compliance with DOD's interim final rule will be a significant barrier to small businesses engaging in the federal acquisition process.

Advocacy has received input from the small business community and cybersecurity experts that the cost of compliance is the single most pressing problem associated with the interim regulation.

---

[9] 80 Fed. Reg. 81472 (December 30, 2015).
[10] 5 U.S.C. § 603(c)(1-4).
[11] 80 Fed. Reg. 81472 (December 30, 2015).

For small businesses, the compliance cost may be viewed through two separate compliance lenses.

1. Small Business Prime Contractors

In the first lens, the small business prime contractor with DOD will clearly be required to implement the requirements of NIST SP 800-171, according to the interim rule. Compliance for these small business prime contractors is very expensive as many small businesses will be forced to purchase services from outside vendors to provide "adequate safeguards" for covered defense information. Most small businesses have neither the technical expertise nor the information technology personnel or software to conduct these services in-house.

Software. The interim final rule will force small businesses to purchase additional software from third-party vendors, and will require small businesses to purchase any annual updates to that software thereafter. For example, cybersecurity experts have told Advocacy that small businesses will need to purchase software for tracking employee computer activity to fulfill the configuration management requirements.

Infrastructure. The interim final rule will force small businesses to purchase services from third-party vendors to fulfill the infrastructural requirements. For example, small businesses will be required to create redundant systems such as off-site, back-up servers for data retrieval in case of a cyber-incident. This costly service cannot be completed in-house by the vast majority of small businesses and could require contracting services from multiple vendors. Cybersecurity experts have also told Advocacy that small businesses will incur significant costs to establish adequate access controls such as encryption, multi-factor authorization, and separation of duties to prevent malevolent collusion. Specifically, multi-factor authorization would require contracting with an outside vendor and would be very expensive to implement.

Consultation. The interim final rule will force small businesses to seek risk and security assessments from third-party consultants. Small businesses will be required to periodically evaluate their information system and security controls and to reduce or eliminate any deficiencies or vulnerabilities. Cybersecurity experts have told Advocacy that small businesses are likely not cognizant of any deficiencies or vulnerabilities and would otherwise react to vulnerabilities and deficiencies as problems arise. Therefore, small businesses will need to contract with a third-party consultant to adequately assess their information systems and security controls.

Training. The interim final rule will force small businesses to either enroll employees in a third-party cybersecurity training course or contract with a vendor to produce an internal cybersecurity training regimen. Cybersecurity experts have told Advocacy that small businesses will not be able to supply adequate cybersecurity training in-house and will have to enroll employees in a third-party cybersecurity training course. In addition, small businesses will be required to contract with a third-party vendor to produce an internal cybersecurity manual.

2. Small Business Subcontractors

In the second lens, the DOD small business subcontractor may also be required to become compliant with the NIST requirements and the prime vendor may impose additional requirements that are not directly required in the NIST requirements but are required for the subcontractor under the terms and conditions of the DOD contract. For example, the interim final rule requires the contractor, both prime and subcontractor, to provide DOD with notification of a security breach within 30 days of the discovery of such a cyber-incident. Some acquisition experts are suggesting that large prime contractors may require their subcontractors to report such infractions to the prime much sooner than the time required by the regulation.[12] In addition, questions have been raised as to whether small business subcontractors will be required to maintain separate security systems for each of their large prime contractors. Clearly, the intent of this interim final rule is not to expand the burdens on contractors beyond that which is necessary to have compliance with NIST. This comment letter will not explore these types of subcontract issues in greater detail, but the DFARS should have affirmative guidelines in the final rule to address the concerns of the small business subcontracting community.[13]

Conclusions and Recommendations

Advocacy believes the interim final rule will be a significant barrier to small businesses engaging in the federal acquisition process, as small businesses will need to expend significant capital to establish adequate cybersecurity safeguards in accordance with the interim final rule.

Advocacy strongly recommends that DOD revisit its initial regulatory flexibility analysis to ensure their estimation of the number of small businesses impacted by this interim final rule includes small business prime contractors as well as small business subcontractors. At a minimum, DOD should provide clarification on the scope of this estimation.

Advocacy also strongly recommends that DOD consider significant alternatives, such as collaborating with universities or other organizations to provide low-cost cybersecurity services to small businesses, or providing a one-time subsidy to small businesses to help cover the cost of initial consultations with third-party vendors.

Advocacy urges the DFARS to give full consideration to the above issues and recommendations. We look forward to working with you as we explore these new opportunities and challenges facing the Federal government in cybersecurity.

---

[12] *See, e.g.,* Phillip R. Seckman, Erin B. Sheppard, Michael J. Mcguinn, CYBERSECURITY AND YOUR SUPPLY CHAIN, Contract Management, February 2016, p.14.

[13] Under section 212 of the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, DOD is required to publish one or more small entity compliance guides for each rule requiring a final regulatory flexibility analysis. Small Business Regulatory Enforcement Fairness Act, Pub. L. No. 104-121, 110 Stat. 847, 858; *see* 5 U.S.C. § 601 note.

If you have any questions or require additional information please contact me or Assistant Chief Counsel Major L. Clark, III at (202) 205-7150 or by email at major.clark@sba.gov.

Sincerely,

The Honorable Darryl L. DePriest
Chief Counsel for Advocacy
U.S. Small Business Administration

Major L. Clark, III
Assistant Chief Counsel
Office of Advocacy

Daniel T. Kane
Law Clerk
Office of Advocacy

Copy to: The Honorable Howard Shelanski
Administrator, Office of Information and Regulatory Affairs
Office of Management and Budget

SBA
Office of Advocacy
www.sba.gov/advocacy