COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22209
703-570-4120

February 29, 2016

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

Re: DFARS Case 2013-D018; Interim Rule Amendment 12-30-2016 on Network Penetration Reporting and Contracting for Cloud Services; CODSIA Case 11-15(a)

Dear Mr. Pitsch:

On behalf of the undersigned members of the Council of Defense and Space Industry Associations (CODSIA) [1], we offer the following additional comments on the Defense Federal Acquisition Regulations Supplement (DFARS) Case 2013-018, entitled, "Network Penetration Reporting and Contracting for Cloud Services," as amended by interim rule changes published in the *Federal Register* by the Department of Defense (DoD) on December 30, 2016.

Introduction

CODSIA submitted a comment letter on November 17, 2015[2] in response to the original version of the interim rule. That letter contained comments to a comprehensive set of cybersecurity issues related to the DoD rulemaking. Those will not be revisited in detail except to the extent that the amended rules now overlap, or create new challenges, with some of the concerns identified in those previous comments. At the time the comment letter was submitted, the most frequently voiced problems raised throughout industry, both by large and small firms, and at an information security forum convened to address the rule, was that the first interim rule was fundamentally unfair because it did not (1) allow sufficient time to address the new security requirements or (2) allow federal contractors enough flexibility or latitude to adapt any of their own existing security protections to the NIST controls required under the interim rule.

Subsequent to the comment deadline, and to their credit, DoD convened an "Industry Implementation Information" day on December 14 to provide further information in the form of a slide presentation and speakers from various DoD functional offices, including DPAP, the DoD

[1] At the suggestion of the Department of Defense, the Council of Defense and Space Industry Associations (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, the American Council of Engineering Companies, the Information Technology Alliance for Public Sector, the National Defense Industrial Association, the Professional Services Council, and the U.S. Chamber of Commerce. CODSIA acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. Combined these associations represent thousands of government contractors and subcontractors. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

2 See http://www.itic.org/dotAsset/4/2/420da80b-931b-425e-ac61-f19b57571208.pdf

CIO and Legal Counsel and to provide a forum to engage with industry on their concerns. Chief among those industry concerns include the following:

1. Implementation should be delayed, postponed or enough time be given to phase in the NIST control requirements to mitigate the threat of contract breach or compliance violations;
2. DoD planned to apply the policy and clauses regardless of whether the contract involved the classes of information subject to the security requirements and it was unclear whether DoD would identify the information subject to the new requirements;
3. Considerable clarity was needed on the CIO engagement process on alternatives or deviations or even why contractors could not rely on their own information security processes and controls rather than seek DoD CIO approval prior to the award of a contract;
4. The rule would further erode the DoD industrial base and increase the number of obstacles to market entry to the DoD supply chain, for small businesses, commercial and COTS providers and new start-ups with innovative technical ideas;
5. Information on how to comply with the NIST controls, especially in the absence of any flexibility to use ongoing best practices or existing security process designed to meet the control;
6. The inclusion of export control information in the definition of CDI and the nature of DoD's authority over export control information versus long-standing regulatory authority in place at the State and Commerce departments over such information.

After the meeting, DoD issued the amended interim rules on December 30. Those rules provided some immediate relief to contractors and subcontractors, primarily but not exclusively, in the following areas:

1. Offerors must now comply with NIST SP 800-171 no later than 12/31/2017;
2. Subcontract flow-down was limited to subcontracts where the work will involve CDI or operationally critical support, but tailoring or alteration of the 7012 clause required to be flowed-down was prohibited;
3. The requirement to receive pre-award approval from the DoD CIO prior to award of any "alternative but equally acceptable security measures" was removed from the 7012 clause (but not from the 7008 clause);
4. Contractors are now required to notify the DoD CIO within 30 days of any NIST SP 800-171 security requirements not implemented at the time of contract award, even though the phase-in of the requirements was authorized.

However, there were relatively few other changes to the policy provisions or the clauses with second interim rule. Industry still has significant concerns with the rules as explained below.

Comments/Concerns:

1. We recommend that DoD conform the first and second interim rules, the multi-factor deviation (now apparently subsumed into the broader compliance phase-in, but not

specifically addressed in the amended rules), and the DoD PGI into a single consistent and transparent network penetration policy;

2. The interim nature of the rules is cause for significant concerns. CODSIA commented at length in our previous letter about how issuing an interim rule to immediately implement evolving and unstable set of controls, and without prior dialogue with industry, was ill conceived. Most DoD contactors were unprepared for the mandate to immediately implement all the NIST controls. Many of the contracts were the result of solicitations issued long before the August interim rules were released. The new clauses were thrust upon many potential contractors as a last step prior to making the award and without the ability of the contractors to price out the performance and compliance requirements for the period of performance or to make a claim that the new requirements were not part of the contract price.

   Contracts issued between August and December 30, 2015 contain early versions of the operative clauses which require immediate compliance with all the NIST SP 800-171 controls, where presumably contracts issued after December 30 will contain the amended phase-in requirements allowing companies until December 31, 2017 to attain full compliance. Where offerors agreed to the August 2015 version of the clauses, DoD has advised that contractors should negotiate relief, if needed, from any performance or compliance requirements pursuant to the first interim rule clauses with individual contracting officers.

   We recommend that, in lieu of each contractor attempting to negotiate the phase-in relief provided in the amended rules on every transaction, DoD issue a block change modification to the interim rules designed to modify all contracts where the relevant August interim rule clauses are present and adopt the December 30 changes. It is fundamentally unfair to issue interim rules where the basic requirements were of such a controversial and fluctuating nature, subsequently and shortly thereafter provide for phase-in of the requirements through 2017, and not make those amended rule changes automatically retroactive to all active contracts issued between August 26 and December 30, at least where full compliance is not required until December 31, 2017. This would relieve contractors from fending for themselves with each CO in DoD, which will likely result in inconsistent and conflicting obligations among DoD contractors and subcontractors on contracts issued under the first interim rule. We further recommend that a safe harbor be granted to any contractor from any false statement or false claims act liability where a contract containing the August version of the interim rule clauses was inserted into the contracts prior to award.

3. As a threshold matter, the requirements in the compliance representation clause (7008) and the security requirement clause (7012) clauses are fundamentally at odds with respect to how exceptions to strict contractor compliance with NIST SP 800-171 are to be managed and administered. DoD must clarify the distinctions between how a requirement variance process from the NIST controls required in the 7008 representation clause (a written explanation and adjudicative process by the DoD CIO

pre award) differs from the security clause at 7012 (that allows for phased-in implementation with a process of proposing alternatives without pre-award approval), notwithstanding that CODSIA supports the flexible use of contractor alternatives on their own determination, and not based on DoD concurrence or approval at this stage of the implementation (see below),

As such, there is confusion about DoD's deletion in the second interim rule over the requirement to obtain pre-award approval from the DoD CIO in the use of "alternative" security measures. In lieu of pre-award approval, the clause requires notice within 30 days by a contractor and ostensibly all subcontractors of any security requirement in NIST SP800-171 not implemented at time of award. The notice is meant to inform DoD about which parts of NIST SP 800-171 a contractor and subcontractor may not be in compliance with, but in any case, does not require the contractor to submit an alternative, while the next paragraph addresses how an alternative to *any* security control must be "accepted in writing" by the DoD CIO.

While the relief from the requirement that any alternative to NIST SP 800-171 be approved at the pre-award stage is a good step, the requirement to give notice within 30 days creates confusion about a process where a contractor or subcontractor is already using alternative measures to meet NIST SP 800-171 controls.

First, such a notice is dependent on whether the contractor or subcontractor has performed a self-assessment or gap analysis of their NIST SP 800-171 compliance; if they have not, 30 days is insufficient, especially those in the first stages of implementing IT systems security, including small businesses. Even where a contractor has done a gap analysis, 30 days may not allow enough time to prepare proper documentation of alternatives, especially where the contractor or subcontractor have multiple sites subject to the rules. This requirement should be modified to allow at least 90 days after award, and DoD should allow for a single corporate-wide compliance for all contractors that wish to do that, especially where a corporate compliance reflects attention to the security of their information systems at the highest level in a corporation. In any case, such a compliance requirement could be accomplished at annual or semi-annual intervals, and not on every single transaction within 30 days, so it does not place too large a cost burden on DoD on its contractors.

Second, DoD should allow contractors to determine over what controls apply and whether any alternative method is sufficient to meet the control requirements for their information systems without inserting further DoD acceptance, approval or adjudication authorities along that path. Provided an offeror/contractor already has a cyber-security compliance plan demonstrating the ability of that plan to meet the NIST or even higher level requirements or controls, they should be presumed to be in compliance with any control or set of controls when *representing* in the 7008 clause that any alternative security measure meets an underlying NIST requirement. There is no need for further steps to adjudicate, approve or document any alternatives.

While industry agrees that implementation of the new cybersecurity security requirements is needed to prevent damage to government and contractor interests, we question the purpose of any post-award notice to DoD about the current state of any contractor information system where the underlying NIST requirements are not required to be in place until December 31, 2017 or the contractor has alternatives in place to meet the control requirements. For example, what is the purpose of a contractor representing in an offer that they will be in compliance with the controls by December 31, 2017, but the contract performance period expires before December 31, 2017? An alternative to a pre-award representation and post-award notice process is that the operative clauses and/or the notice requirement could be made applicable only to contracts whose period of performance is not complete until after December 31, 2017.

Third, implementing NIST 800-171 may take longer than anticipated by this rulemaking; even with an extension of the compliance date, there is a possibility that even after December 31, 2017, contractors may need additional time to address all of the NIST controls. CODSIA recommends that a process be instituted that would allow a review by the DoD CIO of such requests after the deadline has passed.

4. DoD should expressly clarify that any costs to implement the NIST security controls requirements per the contract clauses are allowable under FAR Part 31 and DFARS 231;

5. Thus far, DoD contracting officers have been reluctant or unequipped to make the decision that the contract contains CDI subject to the clauses or, conversely, out of an abundance of caution then apply the clause to every DoD solicitation without regard to whether the resultant contract should be made subject to the clauses.

   DoD contracting officials should make it absolutely clear in solicitations and other relevant documents at all points in the acquisition process, including contract formation and post-award management, that the requirements include CDI subject to the network penetration rules. If notice is not given up-front in the solicitation process that the requirements will apply, the contractor should not be subject to any post-award failure to apply their internal systems controls to that contract we do not believe it would be or should be enforceable. The NIST requirements cannot be implied under any type of circumstantial analysis, nor should the contractor be left to decide whether the security measures or the reporting requirements apply. Consistent with the PGI, which states that CO's will identify CDI, industry recommends that a prominent notice that the clauses apply to the requirements into every RFP prior to issuance.

   If anything, the public meeting created more confusion than clarification about inclusion of the clauses. At several points in the meeting, different answers were given about how offerors were to be given notice that the contract contained requirements subject to the rules, including the observation from DoD that contractors "will know it when they see it" and that any clause would be self-deleting if they did not apply to a specific requirement. Obviously neither of these answers is helpful where information security

is implicated, the costs to implement the controls can be prohibitive, and the contract proposal and performance risk is high without effective notice prior to award or any subsequent modification that the contract will contain CDI.

6. Flow-down changes

   a. CODSIA continues to recommend that DoD exempt contracts for commercial and COTS items from application of the Final Rule or, in the alternative, exempt subcontractors supplying commercial or COTS supplies or services from flow-down of the final rules. If commercial items are not excluded in the Final Rule, we respectfully request clarity as to which data fields of the SF1449 are considered "covered" and which are not. We need to know precisely, so we can protect the data in accordance with the 800-171.

   b. Prohibition against tailoring – DoD contractors apply any number of legally enforceable methods to achieve the requirements of their contracts and flow-down risk and compliance requirements to their subcontractors, including the commercial or COTS supplier base, which we believe should be exempt. Where a FAR or DFARS, or other agency supplement makes the flow-down mandatory, most federal primes include those clauses verbatim in subcontracts so that complete flow-down compliance can be managed and enforced at the subcontract level to the parties satisfaction. Where not mandatory, each prime contractor applies any number of tailored contract terms and conditions to insure subcontractors meet requirements. As such, CODSIA recommends that DoD revert to the subcontract flow-down language in the first interim rule that did not prohibit tailoring of the clauses.

   c. Where DoD requires flow-down without alteration, can industry assume that wherever the language in 7012 refers to a "contractor", the term "subcontractor" should or can be used in the flow-down version of the clause, except where "subcontractor" is already used in the claus? We recommend further that where subsection (m) (2) requires cyber incident reporting to "DoD…and the prime contractor", the term "(or next higher tier subcontractor)" can be appended after "prime contractor".

7. Where the 7012 clause defines the security requirements as NIST SP 800-171 (Subsection (b)), but requires notice to the DoD CIO through an unencrypted email, it creates serious concerns about disposition of such confidential information. Disclosing unimplemented requirements seems to hold some risk to the disclosing contractor or subcontractor given that revealing what security measures have not been implemented and whether there is a proposed alternative, could open companies up to risk of exfiltration outside of DoD of relevant contract CDI. This approach could create heightened vulnerability due to the disclosure itself where disclosure is given over an email channel that may not have the necessary security attached to them. It is not inconceivable that a disclosure at an unsecured entry point (an unencrypted email

server) could allow malicious actors access to contractor information systems should the vulnerabilities of each contractor or subcontractor be disclosed openly.

We recommend that DoD insure that there are appropriate levels of protection, so that information about unimplemented NIST SP requirements remain secure from any unauthorized access. DoD is attempting to put a non-disclosure requirement into contracts through the 7009 clause to protect information provided in a cyber incident report due to penetration of a contractor's networks and note that third party contractors are prohibited under that clause from revealing relevant contractor disclosures subject to civil and criminal penalties. We recommend that, absent an encryption regime for information about unimplemented controls, and notwithstanding the recommendation above to reconsider or modify the notice process altogether, DoD insure appropriate remedies where any unauthorized disclosure of information subject to the notice requirement takes place and where escape of any submitted can be attributed to a lack of security at the DoD portal.

Aligned with the recommendation above that DoD should change the 30-day notice process to a presumption of compliance where alternates are offered, or alternatively modify the notice to 90 days, we recommend that any notice be authorized to be done through corporate compliance and not on a transactional basis. The rule should also establish a standard for what the information required under any notice process should consist of.

8. Definitions

   a. Critical information (operations security) – DoD should clarify the meaning of terms and explanations given at the public meeting that may have blurred the lines regarding CDI that is critical information operations security. As set forth in the slides provided on December 14, operationally critical support was described as:

      "Supplies or services designated by the government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

      Operationally Critical Support is an "activity"– not an information type – performed by the contractor. ***DFARS does not require protections for contractor information systems that are used to provide operationally critical support – only the requirement for the contractor to report a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support.*** (emphasis added)

      Operationally Critical Support is not related to "Critical information (operations security)"

The slides categorized a large number of activities as "Operationally Critical Support" which expands the number of activities beyond that which might reasonably be considered to generate CDI under the rules and that would require use of the NIST SP 800-171 controls.

b. Covered Defense Information – Identifying controlled defense information will be a significant challenge, as the interim rule does not mandate that DoD mark all of its own data. Complicating matters in many cases is the expansive definition of CDI, which makes it difficult for contractors and subcontractors to accurately and consistently identify. The fourth category of CDI, "Any other information…that requires safeguarding…" appears to include essentially any piece of information not in the public domain which then must be treated and protected as CDI under this interim rule. This is an overbroad approach. In particular, how does this apply to design data for components that are used in both military and non-military applications? For example, if an engine part is on a military aircraft that is developed under a contract that requires all design data to be protected as CDI, and the part is also used on a commercial aircraft, that currently means the commercial aircraft data must now be protected using these rules, because there is a piece of CDI involved.

Controlled technical information" – definition should be updated to remove the vague references to technical information and align with the response provided at the Industry Implementation Day. The definition should be updated to include only the technical information that is marked with Distributions B-F by the DoD.

9. Contracting for Cloud Services:

a. DFARS 252.239-7010, "Cloud Computing Services," sets forth a number of requirements that commercial cloud infrastructure (i.e., IaaS) providers will not be able to sign up to (as primes or subcontractors) because compliance with those requirements are outside of their control; compliance with those requirements falls within the control of the managed services providers, account owners, lead systems engineers, or prime contractors (the "primes") running DoD workloads and storing "government data and government-related data" in the cloud infrastructure. For example:

i. DFARS 252.239-7010(b)(3) requires that all Government data that is not physically located on DoD premises be maintained within the United States or outlying areas. IaaS providers offer cloud regions both within and outside of the United States and outlying areas. It is the responsibility of the primes to select the appropriate region in which to store and process government data. It is inappropriate to assign to IaaS providers, who do not move customer data from one region to another and who do not have any visibility into whether data that the primes store and process on their infrastructure is government data, any liability for ensuring that government data stays within the United States.

ii. DFARS 252.239-7010(b)(2) requires contractors and subcontractors to "implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG)." IaaS providers will offer cloud regions and cloud services that comply with the SRG; however, it is the prime's responsibility to select the region and services that have received an SRG authorization appropriate to the impact level of the Government data, and to attain authorization from a government Authorizing Official to use regions and services that are not SRG compliant.

iii. DFARS 252.239-7010(d) requires that all cyber incidents be reported through the DoD-DIB Cyber Incident Reporting and Cyber Threat Information Sharing Portal, or DIBNET. Primes, and not IaaS providers, will manage the DoD systems running on the IaaS and, therefore, retain responsibility for conducting system monitoring and any pertinent incident response activities, with support from the IaaS provider as requested. IaaS providers will notify primes of security breaches, but, without insight into the nature of the data the primes are storing and processing in the infrastructure, IaaS providers will not know whether a breach results in a "cyber incident," as that term is defined in the clause. Thus, the DIBNET cyber reporting requirements should not apply to IaaS providers, but to the prime using the cloud. *See also* related comment 9(g) below.

iv. DFARS 252.239-7010(f), (g), and (h) set forth media preservation, forensics, and cyber incident damage assessments. Primes, and not IaaS providers, are generally responsible for satisfying these requirements; primes have the ability to generate forensically sound snapshots of their IaaS usage and associated network traffic for forensics and assessments.

v. DFARS 252.239-7010(i)(1) and (2) require that government data be maintained in a particular format and disposed of according to Government instructions. IaaS providers neither format nor dispose of government data.

vi. Although physical access to infrastructure (e.g., data centers) is within the IaaS providers' control, IaaS providers will not agree to DFARS 252.239-7010(i)(3), which provides that a government contracting officer may require physical access to data centers for purposes of audits, inspections, or other similar and undefined activities. IaaS providers, who maintain strict data center access policies for security purposes, generally limit third-party access to data centers to accredited FedRAMP third party assessment organizations and to law enforcement activities. CODSIA recommends that the DFARS should be revised to reflect this practice.

b. While the NIST 800-171 compliance date has been extended to 2017, contractors are still required to notify contracting officers within 30 days of award whether or not they comply. In order to affirmatively state yes/no,

contractors must have completed their review/audit of their systems. It is unlikely that a majority of CSPs have completed such reviews, especially when the government has not given contractor sufficient guidance in terms of whether a third party audit/compliance review is necessary or whether contractors can self-certify. Thus, contractors are likely to do what CSPs would have to do tell contractors that we believe services within CSPs FedRAMP boundary comply with NIST 800-171; however, CSPs are still completing their formal review. These types of answers do not provide the government with useful information, but they do place an additional reporting burden on contractors. There is simply not enough value in the information likely to be obtained to justify the burden placed on CSPs.

c. Companies that have demonstrated compliance with DOD Impact Level L4/5 (as described in the DISA Cloud Security Requirements Guide) should automatically demonstrate that they meet the DFARS Interim Rule requirements. Those CSPs should be able to do so without having to do all the paperwork and without any implied requirement for an additional assessment. Meeting DOD Impact Level 4/5 requirements exceeds the DFARS requirements. This is clear from the draft. Unfortunately, the connection with using a compliant cloud is not specified.

d. CSPs should only be responsible for reporting to customers about incidents that result in an actual or reasonably suspected unauthorized disclosure of Customer Data. As a service provider, the CSP is responsible for managing its infrastructure and security practices. When an incident is impactful to a customer, the CSP is responsible for reporting it. Other non-customer impacting incidents should not be reported to customers.

e. Scoping the reporting requirements to include only incidents that result in an actual or reasonably suspected unauthorized disclosure of Customer Data will enable the DOD to focus on the most impactful and meaningful types of incidents. If CSPs were to report all incidents (and potential incidents), then the effort of reviewing and understanding those would be extraordinarily taxing on DOD resources. As was documented in the April 2014 GAO *Report to Congressional Requesters on Information Security: Agencies Need to Improve Cyber Incident Response Practices*, U.S. agencies likely do not effectively or consistently respond to detected incidents in about 65 percent of reported incidents. According to NIST SP 800-61, *agencies are to consider impact for prioritizing incident response activities*, *such as the fundamental impact of the incident* and the current and likely future impact to business functions. As the GAO report explains, “resource limitations at agencies are one of the factors emphasizing the need for them to prioritize their incident response activities. Further, by prioritizing the handling of incidents, agencies could identify situations of greater severity that demand attention.” Consistent with NIST SP 800-61 and the GAO report, DOD should focus on breaches, which have much

greater impact on DOD than the broader category of incidents or potential incidents. (Reference pg. 11 of this GAO report.)

f. If the reporting requirements are scoped to incidents that result in an actual or reasonably suspected unauthorized disclosure of Customer Data only, then the 72-hour reporting window is reasonable. The clock for notification should start when CSPs have analyzed an incident and 1) determined that the incident is within the reporting scope and 2) determined the scope of the incident (HIPAA, CJIS, financial institutions, etc.).

g. CSPs have a direct relationship with their customers. As such, communication of security incidents should be limited to between the CSP and the customer. Limiting communications from the CSP to the customer is necessary for contractual reasons to ensure that customer data is protected and not shared with third party entities. The customer is responsible for identifying a customer point of contact to be notified in the event of an incident, which could include Agency Security Points of Contact (i.e. Agency Incidents Response Teams, Authorizing Officials). In sum, CSPs should only be required to notify DOD customer tenants individually of within-scope incidents that affect their customer data.

h. Once the customer has been notified of a security incident, the customer can then report the security incident to third parties that they have a responsibility to report to (such as US-CERT or the FedRAMP PMO). These are contacts that are designated/mandated by the customer for security incident reporting. The customer is directly responsible for reporting to these third party entities. In sum, CSPs should not be required to report incident information to a central DOD authority. In addition, CSPs should *not* be required to report incident information via the DiBnet portal because access to the DiBnet portal is limited and challenging, and the flow of breach information should not be interrupted.

i. DOD should align the Interim Rule's reporting requirements with federal-wide efforts rather than prematurely spinning off its own requirements, which may ultimately be supplanted by federal initiatives. In particular, the recently announced Cybersecurity National Action Plan (CNAP) seeks to improve cyber incident response. A policy for national cyber incident coordination and an accompanying severity methodology for evaluating cyber incidents and breaches could help to ensure an appropriate and consistent level of information sharing and response.

10. Can DoD activities or CO's require immediate compliance despite the interim rule phased-in implementation: what does the term "as soon as practical" mean in 7012(b)(1)(ii)(A)? Will individual CO's be authorized to demand immediate compliance with all NIST controls from all offerors in a competitive environment based on their own

judgment about the need and/or make such 100% compliance a condition of responsiveness to a solicitation that can then be used to eliminate offerors from a competitive range or as a source selection discriminator. We urge DoD to make sure any final rules prohibit source selection exclusions based on a desire or demand for 100% NIST SP controls compliance at time of solicitation or contract prior to December 31, 2017.

11. In coordination with the SBA, Commerce and other relevant executive agencies, DoD should establish policy and training mechanisms and learning centers that allow access to the necessary resources to assist small and commercial businesses in creating compliant information systems.

12. International Security Compliance Coordination: DoD should coordinate a dialogue with industry about how the NIST controls may work or not work with other international information control systems and describe how to conform information from the international supply chain into the NIST model.

Conclusion

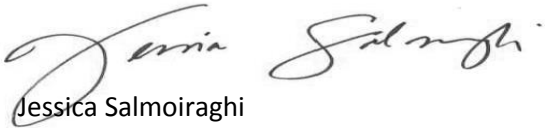
In conclusion, CODSIA requests that DoD respond to the significant number of comments that were submitted previously on the first interim rule if they have not already been addressed, and now address further concerns on other aspects of the second interim rule. The volume of comments alone indicates significant flaws with the rule. In addition to our comments provided herein, we have also included a list of questions that contractors are struggling with in *Appendix A*. The government should consider delaying implementation of the entire rule or suspending it altogether until the government is able to thoroughly review and consider all of the comments submitted.

***

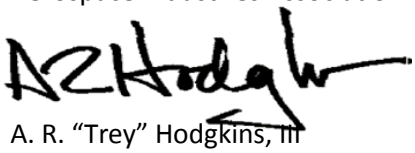
We thank you for your attention to our comments and your consideration of our recommendations. Should you need further information, please contact Pam Walker of the IT Alliance for Public Sector (ITAPS), who is serving as the CODSIA Case Manager for this submission. Pam can be reached at 202-626-5725 or at pwalker@itic.org.

Respectfully submitted,

John Luddy
Vice President,
National Security Programs and Acquisition Policy
Aerospace Industries Association



Jessica Salmoiraghi
Director, Federal Agencies and International
Programs and Acquisition Policy
American Council of Engineering Companies



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

Jimmy Thomas
Director, Legislative Policy
National Defense Industrial Association

Alan Chvotkin
Executive Vice President & Counsel
Professional Services Council

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

APPENDIX A

Questions for the Record

We offer the following questions for inclusion in this activity and encourage the Department to publish the responses in the FAQs addressing this Interim Rule with answers as soon as possible, as contractors and subcontractors continue to struggle with implementation.

1. In NIST 800-171, Appendix E lists four categories of controls (with "tailoring symbols" of NCO, FED, NFO, and CUI). Does being "in compliance" with NIST 800-171 mean that a contractor is compliance with all the control requirements in Section 3 only, or does it mean they are in compliance with the controls in Section 3 and Appendix E (and if so, which categories of controls within Appendix E)? As we are creating our mapping of controls to determine if we need to ask for any alternative/equivalent controls, we're trying to understand if we need to add any of the Appendix E controls into that mapping, and if so, which categories.

2. **252.204-7008(c)(1-2) and 252.204-7012(b)(1)(ii)(A – B)**
   Both of these sections include the extension until December 31, 2017. Does this extension still allow the Contracting Officer to approve alternate/equivalent controls that will be in place after December 31, 2017? Or are they saying you must comply with all the NIST 800-171 controls by December 31, 2017?

   Both of these sections have different timelines and methods for submitting information about which NIST 800-171 controls cannot be met (prior to contract award and within 30 days of contract award). Is the intent to have two separate notifications and approvals, or if the initial notification is completed prior to contract award, does that count as well for the submission that is required within 30 days of contract award? What if the approval is given for one but not the other?

   The December 30, 2015 Interim Rule extended the period for implementation of NIST SP 800-171 until December 31, 2107. As part of that extension they imposed a requirement to "notify the DoD CIO via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award". (DFARS 252.204-7012(b)(1)(ii)(A)) Commercial companies are not exempt from these requirements and may receive hundreds of orders each month. Does the DoD CIO expect to receive an email with the same status being reported with each order? The status of implementation will not change on a daily basis, and may only change every couple of months. This reporting requirement will be onerous for some contractors and will not provide meaningful information to the DoD CIO. We understand the intent is for DoD to monitor across the industrial base the progress being made in implementing SP 800-171 prior to the deadline of December 31, 2017. Recommendation is to modify the reporting to once per month or 30 days after contract award.

The DoD had previously extended the compliance requirement for multi-factor authentication, does this extension until December 31, 2017 also apply to multi-factor authentication?

3. **252.204-7008(c)(2(ii)**
   What is "prior to contract award"? When would this be in the process? Does DOD CIO office still need to approve if the contractor will be in compliance before the deadline of December 31, 2017?

4. **252.204-7009(c)**
   Does this apply to Cloud Service Providers that are not operated on behalf of the government?

5. **252.204-7012(a) – Definitions of "Compromise" and "Cyber Incident"**
   The new definition of "Cyber Incident" removes suspected cyber incidents, but the definition of Compromise (which is used within the Cyber Incident definition) includes the clause "may have occurred". Are suspected or potential Cyber Incidents that may have occurred required to be reported? Or are only actual cyber incidents required to be reported?