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

November 17, 2015

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; Network Penetration Reporting and Contracting for Cloud Services

CODSIA Case 11-15

Dear Mr. Pitsch:

On behalf of the undersigned members of the Council of Defense and Space Industry Associations (CODSIA) [1], we offer the following comments on the Defense Federal Acquisition Regulation Supplement (DFARS) Case 2013-018, entitled, "Network Penetration Reporting and Contracting for Cloud Services," originally published in the *Federal Register* on August 26, 2015, (the "interim rule"). CODSIA requests that the Department of Defense ("DoD," or "the Department") suspend the implementation of the interim rule until addressing the substantial issues we raise in our comments below and immediately implement a broader class deviation discussed in our comments to allow for a phase in approach.

Introduction and Executive Summary

The interim rule has two essential policy and procedural components: (1) safeguarding covered defense information and enhanced cyber incident reporting, and (2) procuring cloud computing services. The interim rule modifies and significantly expands the existing Unclassified Controlled Technical Information (UCTI) policy, replaces the UCTI clause with a set of revised and new clauses and adds a new section on cloud computing. The interim rule applies to all contractors, including small business and where commercial or COTS supplies or services are being acquired under FAR Part 12, and subcontractors, including subcontracts for commercial or COTS supplies or services.

The interim rule establishes a set of baseline security controls for safeguarding purposes, but adopts many new terms of art, including, but not limited to, "compromise", "cyber incident" and an expansive definition of "media." Moreover, the interim rule uses extremely broad and

[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.

vague terms such as "potentially adverse" and "may have occurred" to set a compliance standard that do not help contractors and subcontractors to define how to meet their reporting obligations, nor provide clarity around their investigation obligations. Suffice it to say, the complexity of hitting such a fast-moving regulatory target has overwhelmed the capacity of many in industry and government to comprehend all of the nuances and highly technical language of the governing information technology (IT) and system governance principles and while this new interim rule represents a step towards addressing the threat, it does not dramatically enhance industry's understanding of the fundamental issues.

Complicating matters further is the fact that the federal government is concurrently attempting to regulate cyber-space through on-going rulemakings and guidance documents at the Office of Management and Budget (OMB) (agency acquisition principles), National Archives and Records Administration (NARA) (Controlled Unclassified Information – CUI), within the underlying defense industrial base (DIB) information assurance infrastructure (applying the DFARS rules to the smaller DIB population), Intellectual Property Enforcement Center (IPEC) (protection of industry intellectual property from trade secret theft), National Institute of Science and Technology (NIST) (cyber risk management voluntary framework and standards for internal controls), and as part of the implementation of Executive Order 13636 of 2013, which in Section 8(e) assigns overall functional acquisition rulemaking responsibility to the joint DoD-General Services Administration (GSA) 8(e) Working Group (cyber-security acquisition risk management framework). The FTC, the SEC and the FCC have also all independently promulgated separate cybersecurity rules and guidance in recent months. These efforts are creating a patchwork quilt of regulatory standards. While all of these documents and rules are prudent actions taken to protect the cyber ecosphere, the sense in the private sector is that agency actions are not being coordinated effectively and their impacts all create different challenges.

DoD had an existing cybersecurity safeguarding regime, including a contract clause entitled Safeguarding of Unclassified Controlled Technical Information, set up in the DFARS at 252.204 and 239 respectively and only completed the rulemaking in late December of 2013, but that regime has been subsumed by this new interim rule. Even before we filed these comments, DoD issued a deviation to the interim rule authorizing nine (9) additional months for contractors to meet its multi-factor authentication requirement, clearly acknowledging the inability of industry to comply with at least one of the requirements of the interim rule. Yet even this deviation is insufficient for many companies where 9 months will not allow them to compete their procurement processes and other necessary implementations to be in place within that timeframe. DoD has also promised additional direction to contracting officers through their internal Procedures, Guidance and Information (PGI) system, which is not subject to public comment and will be contemporaneous with this interim rule implementation. This PGI could further complicate how industry interacts with various DoD agencies, which may impose requirements beyond those in the interim rule or interpret the interim rule in ways inconsistent with any final DoD implementation or with industry comments.

Of those other rules in process, many federal agencies are involved jurisdictionally in the regulation of various elements, so industry is being challenged by the amount of regulation being promulgated in the cyberspace. Each one is distinct and focused on some unique

component of the cybersecurity eco-sphere and being executed by agencies all with different missions, policy priorities and agendas. Some of the regulations in the pipeline are consistent with each other and align with national strategic cybersecurity goals. But others are inconsistent with each other or share little in the way of common objectives. We note that industry has submitted thousands of pages of comments to the many rulemakings in progress and is continually scrambling to address the latest rulemaking, while the previous ones go remain in limbo for an indeterminate period and based on unspecified or highly dynamic reasons.

In that context, this interim rule is required by Sections 941 of the Fiscal Year (FY) 2013 National Defense Authorization Act (NDAA), enacted in January 2013, and Section 1632 of the FY 2015 NDAA enacted in December 2014. This interim rule goes beyond the statute's focus for reporting breaches and adds many new requirements. Considering that all commercial organizations worldwide, all businesses and the general public use information systems to conduct their everyday activities, it is reasonable to conclude that this rulemaking will have a significant impact to all American companies, and maybe even the entire global supply chain.

Earlier requests by industry groups to hold a public meeting to clarify DoD intent and educate industry were denied. Although an extension to the comment period has now been granted, prior requests to extend the comment period were rejected, all despite the fact that the interim rule is interim and in force, while the regulations required by the underlying statutory requirement (Section 941) are more than 2 years overdue.

Notwithstanding those procedural concerns about the regulatory process, industry is constantly engaged in addressing cybersecurity protection and adapting their systems and security processes to meet the ever changing and persistent cybersecurity threat. With respect to the regulatory framework being established by submitting to another interim rule, industry respectfully requests that, in due course, all of the component elements of a cohesive cybersecurity strategy be eventually conformed by some agent of government working in concert with industry groups so that the plethora of different regulatory structures can be reduced to a set of sector specific policy frameworks, be aligned with industry business models and the NIST framework, and managed without government or industry having to create separate, irregular compliance schemes and so that the federal acquisition process can be consistent and made repeatable by all agency contracting officials.

This letter goes into great detail on a number of issues CODSIA members have with this interim rule including:

- Immediate effect of the interim rule without public comment
- Changing NIST Standards is not a simple switch for contractors
- Policy Issues
    - Information security requirements
    - Definitions
    - Mandatory flowdowns
    - Subcontractor and supplier compliance

  - Alternative control procedures and contractors submitting deviations to the clause
  - Mandatory cyber incident reporting
  - Identifying and marking covered defense information
  - Contracting for cloud services
  - Access to contractor and subcontractor systems, information, and equipment
- Other concerns
  - Impact on global business and non-federal clients
  - Sharing and protection of contractor and subcontractor data and information
  - Liability Protection for Information Disclosures pursuant to the interim rule's reporting requirement
  - Reconcile requirements with Sec 325 of Intelligence Authorization Act of FY14
  - OMB Draft Guidance on Improving Cybersecurity Protection in Federal Acquisitions
  - Impacts to Small Businesses
  - DoD Oversight

Immediate Effect of the interim rule without Public Comment

As a threshold matter, CODSIA objects that such a significant and important rule was issued as an "interim rule" without prior notice and comment. This interim rule is a significant mandate on contractors and subcontractors and does not provide industry with time to implement the requirements in the interim rule.

The rule was issued as "interim" on August 26, 2015 to implement Sections 941 of the Fiscal Year (FY) 2013 National Defense Authorization Act (NDAA) and Section 1632 of the FY 2015 NDAA and to update and align existing DoD guidance on the acquisition of cloud computing services. Again, this interim rule goes far beyond the scope of these laws. While CODSIA agrees that a secure and reliable cybersecurity infrastructure is needed, implementation of the interim rule creates significant performance and compliance challenges for federal contractors and their supply chains. The recent breaches of federal information systems are potent examples of the need to increase the level of protection, but given current risk assessments by industry security experts, immediate contractor and subcontractor compliance with 109 new requirements referenced in the interim rule is not immediately technically feasible, nor an economically efficient strategy to secure the cyber ecosphere from breaches.

Acceptance of the interim rule is required in virtually all DoD solicitations, contracts and subcontracts and could impose unacceptable risks to contractors and subcontractors of being immediately in breach of contract for non-compliance – or worse – making a false representation of compliance in violation of the False Claims Act (FCA). While CODSIA understands the urgent need to protect Covered Defense Information (CDI) in contractor and subcontractors IT systems, it is unreasonable for them to assume this risk, without adequate time to prepare for assessment and compliance with these new requirements. Given that DoD has already issued a Class Deviation to the interim rule on October 8, 2015 and has now released their PGI (not reviewed at the time of this letter), prior to the due date for receiving comments on the interim rule, it is clear that the new proposed clauses are not ready for implementation on a wide scale as is directed in the interim rule and the Class Deviation.

The October 8, 2015 Class Deviation exempts multi-factor authentication from the underlying NIST framework standards from contractor compliance for up to nine (9) months and makes a request for added time after 9 months a matter of notice to the Contracting Officer (the deviation does not require CO approval for any added time). Unfortunately, the deviation still offers insufficient time to facilitate effective implementation of all of the interim rule's requirements across the entire defense industrial base.

Accordingly, CODSIA strongly recommends that DoD issue a more comprehensive, Class Deviation that permits contractor and subcontractor compliance to the new clauses based upon an assertion made in "good faith" that compliance will be diligently pursued in accordance with all applicable requirements (up to and including the new 109 requirements) consistent with a reasonable timeline and as agreed upon between a Contractor and the Contracting Officer prior to, or during, the course of performance to any contract containing the clauses. Any revised Class Deviation should also flow-down throughout a prime contractor's supply chain and allow for a good faith assertion and similarly tailored timelines between prime and subcontractors for compliance to the clause requirements. We note that even with complete compliance to the existing 252.204-7012 Safeguarding clauses, most of industry will still have to immediately execute to 70 new or revised NIST 800-171 control requirements to comply with the interim clause at time of contract award. CODSIA therefore recommends that DoD consider creating a revised Class Deviation authorizing the parties to tailor the clause as set forth above and that phases in implementation of the interim clause requirements by the end of calendar year 2017.

We share the goals and interests of the government in strengthening our cyber posture because cybersecurity is critical for CODSIA member companies as well. Cyber threats continue to evolve and become more sophisticated. The protection of customers, brands, and intellectual property – which are essential components of CODSIA members' businesses – are critical to their ability to grow and innovate in the future. Member companies seek to maintain the highest levels of integrity in their products and services, regardless of whether they are sold to commercial or government markets. Moreover, as both providers and users of cybersecurity products and services, CODSIA associations' members have extensive experience working with governments around the world on cybersecurity policy, and we are committed to working with the U.S. Government to improve cybersecurity, but believe additional time per the requested deviation process is needed to conform existing federal and private sector practices with the new DoD requirements.

Unfortunately, this interim rule creates many challenges discussed at length herein. The letter consists of principal sections addressing the key policy issues, other significant industry concerns and observations, and specific recommendations to the operative clauses, as well as a list of sample instructive questions in the appendix[2] to be included in the DoD web portal as FAQ's that can be shared throughout the DoD industrial base as the rulemaking process proceeds. In some cases, observations or comments address different aspects of the same policy issues and are addressed at multiple points herein.

[2] The Appendix of Questions for the Record can be found on page 27 of this letter.

Changing NIST Standards is not a simple switch for contractors

DoD has made reference to the existing DFARS requirements regarding unclassified critical technical information or UCTI as facilitating the implementation of these new interim rules by the industrial base. Such a comparison is incorrect, as the change from the NIST SP 800-53 to the NIST SP 800-171 as proposed by this interim rule includes dozens of variants from previous compliance metrics. Based on Table D of the NIST 800-171 document, if a company is fully compliant and had implemented all 60 NIST 800-53 required controls from Table 1 in the November 2013 DFARS clause:

- The company would fully meet 39 of the NIST-171 requirements
- The company would partially meet 22 of the NIST-171 requirements
- The company would have 48 new requirements to deal with
- The net – 64% (70 of 109) –of the requirements detailed in NIST 800-171 are new or "partially" new as compared to the NIST 800-53 controls required by the 2013 DFARS clause (252.204-7012). These new and/or partially new requirements require interpretation, assessment and possible implementation in order to ensure compliance.

Using NIST 800-53 controls to satisfy the 109 requirements from NIST 800-171 would require the implementation of 125 unique NIST 800-53 controls. While there is some uncertainty about the scale of the -53 controls versus the scope of the -171 safeguards in the NIST policy documents, the net number of NIST 800-53 controls required more than doubled from 2013 to the August 2015 DFARS clause (252.204-7012) release.

Policy Issues

a. Information Security Requirements

The modified rule for safeguarding specifies a new set of controls from the November 2013 DFARS Table 1 – Minimum Security Controls for Safeguarding, including the addition of Operations Security and other regulatory requirements at 252.204-7012 (based on NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations). At the outset, it will take time for contractors and subcontractors to assess and comply with the controls specified in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Plans will take time to develop and execute across the enterprise, businesses, and program environment. The initial list of requirements that call for an immediate risk analysis and review are:

- Multifactor authentication for all accounts when accessing networks
- Encryption via FIPS-validated cryptography
- Labeling all physical media with appropriate data classification markings

The controls are vague and open to contracting officer interpretation. A number of the basic and derived security requirements may not be feasible and are rigid to risk aversion, leading to performance degradation, duplication, and inefficiencies.

These comments do not address all the issues in NIST 800-171 and those issues are the subject of numerous other industry comments and submissions. It is immediately evident, however, that the terminology in this interim rule at DFARS 252.2004-7012 is inconsistent with NIST 800-171. It is unclear why DoD declined to use the term "Controlled Unclassified Information" in the interim rule, particularly when it references the security protections of NIST SP 800-171, which specifically apply to both contractor systems operated on behalf of the government and internal contractor/subcontractor business systems that store government CUI data. This interim rule must be reconciled with the government-wide CUI guidance. At a minimum, CODSIA recommends that no final rule be issued until such time as the terminology in this interim rule is conformed to the terminology of NIST 800-171, which is intended to be the controlling, government-wide requirement on this topic

b. Definitions

Additionally, we find many problems and challenges with the following definitions in the interim rule:

"Compromise"

- This term could be interpreted to include situations that industry would not consider to be a network/system *compromise* as that term is commonly understood (e.g., copying CDI to unauthorized media, loss of computer equipment, inadvertent deletion of files from a server, and other similar events…) Put differently, violation of an IT security policy does not equal compromise of a computer network or information system.

- The term as used would cover situations where someone was inadvertently given access to CDI, even if they didn't actually access the information.

- Does DoD intend to establish a disclosure obligation for CDI similar to that for ITAR-controlled information? If so, there is no infrastructure for such a scenario in place.

- The definition includes loss of an "object", which may require contractors to investigate, preserve, report, and possibly produce laptops and mobile devices that store CDI. Such steps would seem to be unnecessary when CDI is stored on a device using embedded encryption (whole disk encryption for example).

"Contractor attributional/proprietary information"

- The definition encompasses more than just CDI and exceeds the stated scope of the subpart (see 204.7300), namely, "to safeguard covered defense information that resides in or transits through covered contractor information systems…."

"Covered defense information"

- The term includes a number of categories of information, and appears to encompass proprietary information that is neither technical data, nor computer software. Furthermore, the definition of Covered Defense Information is expansive, requiring data to be safeguarded without clear marking instructions and identification of operational processes. While, in some cases, it is clear that information would fall within one of the categories, such as information specifically marked or delineated in the contract, in other instances, it is not clear. For example, where a contractor receives or generates information in the course of contract performance, it may be unclear whether it falls within a given category (e.g., information "vitally needed by adversaries for them to plan and act effectively…") or relies on marking instructions on Contract Data Requirements Lists (CDRLs), which specifically require Government instruction as to the type of protection or encompasses financial data included in a CDRL (DoD Instruction 5230.24 instructs that the assigning of a specific statement is an "inherently Governmental responsibility").

- With respect to the transportation industry, these ambiguities are particularly concerning. For example, it is not clear whether basic information about the identity of who ships a package, who receives a delivery, and where a delivery is made would fall within the definition of "Covered Defense Information." The answers to these questions carry significant implications for the industry. Member companies engage in millions of transactions each day that involve shipment-specific details. In the vast majority of instances, this detail is not sensitive, but is still protected in accordance with industry standards. Broad application of DoD safeguarding and reporting requirements to this type of information would require contractors and subcontractors to incur significant expense with few, if any, resulting benefits. Such an approach is untenable in the industry and seems inconsistent with the intent of the interim rule.

"Critical Information"

- The definition of "critical information" under the Operations Security process can differ among commands and DoD entities, thus it is not clear from the interim rule which standards to apply to determine whether an item is "covered defense information." Where it is not clear whether information constitutes covered defense information, what is the process for obtaining clarification from the government? Moreover, what is the process for determining whether information is "critical information" under the Operations Security process? The addition of Operations Security and other regulatory requirements generalized into broadened categories (i.e. CUI, PII, and EXIM) through conflicting laws and regulations will introduce operational inefficiencies and baseless redundancies. Any process should be appropriately centralized to ensure that information is treated consistently across contracts and DoD entities. Further, what standard is applied to determine

whether a contractor or subcontractor reasonably complied with the interim rule when determining whether specific information falls within the requirements?

"Cyber incident"

- The interim rule significantly expands the definition of a "cyber incident" in DFARS 202.101 as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." The cyber incident reporting requirement at DFARS 252.204-7012(c)(1), however, only requires the reporting where a cyber incident "affects a covered contractor information system or the covered defense information residing therein…". Thus, it is not clear whether cyber incidents with potentially (i.e., not actual) adverse effects must be reported and whether such reporting is required where the incident affects or potentially affects only non-covered defense information in the covered contractor or subcontractor information system. Importantly, requiring contractors and subcontractors to report "potentially adverse effects" will place a significant burden on both the government and contractors/subcontractors, particularly since it is not clear what is meant by a "potentially adverse effect" and this term may be construed very broadly. If contractors and subcontractors are required to report all "potentially adverse effects" they may be required to incur significant expense to report thousands of innocuous incidents. Without further clarification, there is potential to create a substantial burden for contractors and subcontractors with no commensurate benefit for the government. Accordingly, the clause should address: (1) what is meant by the term "potentially adverse effect" and what factors/elements should contractors/subcontractors evaluate when determining whether an incident falls within this definition; (2) whether contractors and subcontractors must report cyber incidents with a potentially adverse effect or only those that have an actual adverse effect, meaning actions that are likely to result in exfiltration of CDI or installation of unauthorized command and control capabilities or, (3) in the alternative, remove the word "potential" from the clause.

.

"Export Control"

- The interim rule's definition of "export control" is quite broad and does not explicitly exclude publicly available information or fundamental research. "Export control" is limited to the export of a wide variety of items "whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives," but the interim rule does not provide guidance on how the public should interpret this limitation. The definition of "export control" is drafted in an unclear and overbroad fashion, stating "dual use items; items identified in export administration regulations, international traffic in arms regulations, and munitions list; license applications; and sensitive nuclear technology information." The interim rule includes imprecise terms like "license applications" and provides no citations to the U.S. export control regulations to

which it appears to be referring (e.g., 22 C.F.R. Parts 120-130). We recommend that the Department consider an alternative definition along the lines of "*Unclassified information that is technology specified on the Commerce Control List in the U.S. Export Administration Regulations and controlled for national security (NS), nuclear proliferation (NP), missile technology (MT) or chemical and biological (CB) control reasons, technical data specified on the U.S. Munitions List in the International Traffic in Arms Regulations, or sensitive nuclear technology set forth in the Department of Energy's regulations at 10 CFR § 810.*"

c. Mandatory flowdown

The interim rule creates a flowdown of requirements throughout the defense supply chain that may lead to unintended consequences. The mandatory flow down of requirements in the NIST SP 800-171 standard requires all companies throughout the supply chain to significantly upgrade cyber capabilities. These costly expenses will have a particularly burdensome effect on small- and medium-size business. Given commercial business sales practices, commercial companies often do not know who the end customer is and, among other things, commercial entities will have challenges complying with the DFARS interim rule.

The flowdown requirements apply not only to subcontractors at any tier, but even those subcontractors that sell commercial items. Applying such DoD-unique regulatory burdens on commercial vendors creates a disincentive for those vendors to stay in the defense market and erects substantial barriers to new entrants. The effectiveness of this mandatory flow-down to commercial suppliers is negligible at best, as stated above, because many commercial vendors may not even realize that their products are being procured for DoD or U.S. government-purposes. They sell their products through a series of distributors and resellers and often have no way of knowing or finding out the identity of the end customer. In fact, we strongly feel that applying this clause to commercial items may negatively impact the Department's commercial item outreach activities, including the Defense Innovation Initiative, and undermine any progress from Secretary Carter's visits to Silicon Valley and the strong preference he has indicated for leveraging innovation developed in the private sector.

CODSIA thus recommends 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 the final rules.

d. Subcontractor and Supplier Compliance

Considering the disclosure, reporting and access requirements of the interim rule, we also note that even with carve-outs for commercial item providers, it will be extremely challenging for prime contractors to ensure subcontractor's compliance with the security, system and reporting requirements. Prime contractors have historically been limited or restricted for many reasons from auditing or having free access to subcontractor systems for

purpose of ensuring complete end-to-end contract compliance and have not previously been successful in getting access to proprietary or sensitive systems at subcontractor's facilities. Even were such access a possibility, prime contractors do not desire to "manage" subcontractor compliance with cybersecurity requirements, due to the increased risk and cost associated with such managerial functions. Typically, subcontractor certification to the prime contractor to their compliance in a subcontract transactional environment is legally sufficient for purposes of administering the subcontract and addressing risks. These technical requirements will create compliance challenges for all sized companies, including large contractors.

Among other things, concerns about duplicate or conflicting subcontract incident reporting have not been addressed and those could lead to a high risk of liability to the prime contractor for either subcontractor non-performance or non-compliance or both. Failure of a subcontractor to meet their duty to report or simply not have the required security protections in place as required in the clauses creates enormous risk for any prime contractor, regardless of size, and such failure could financially harm even the largest companies. Such concerns create valid policy questions about risk mitigation and CODSIA suggests that the Department open a broader discussion with industry and other stakeholders prior to any final rule to consider an alternative risk mitigation structure consistent with the NIST framework.

Accordingly, and in the absence of any joint industry-DoD meeting on risk mitigation management, CODSIA recommends that a liability safe harbor indemnifying prime contractors and subcontractors at any tier in the supply chain subject to this interim rule from contract and other damages related to a breach event should be establish in the final rule, conditioned on the good faith effort by a contractor to meet the compliance requirements. Such a means of achieving indemnification would allow contractors relying in good faith on subcontractor certifications that they are in compliance with the clause requirements and a risk-based framework, to obtain relief from contract and third party liability and be shielded from devastating fiscal consequences set in motion through no fault of their own. Further, such a system would incentivize those in the DoD supply chain to build more robust IT protection systems. At the very least, a SAFETY Act-type liability protection regime should be offered as a way to mitigate risk for federal contractors in the current absence of express application of SAFETY Act liability limits and contract clauses to cyber-security breach incidents. This may require further exploration with government authorities to flesh out the correct approach. If the Safety Act were to be expanded to specifically include cybersecurity activity in its ambit, we recommend insuring that DoD contracting officials be trained in its usage.

DFARS 252.204-7012(m) should be amended to require contractors to "include the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items, **through which the Contractor will provide to the subcontractor covered defense information in connection with the performance of the subcontract**." The vast majority of commercial subcontractors will not receive, collect, develop, transmit, use, or store covered defense information and, therefore, this clause

should not apply to them and they should not be required to institute extensive and costly compliance mechanisms to comply.

e. Alternative Control Procedures and Contractors Submitting Deviations to the Clause

In the interim rule, DFARS 252.204-7008(c)-(d) affords contractors the opportunity to submit a request to deviate from the security requirements in NIST SP 800-171 and states that the DoD Chief Information Officer (CIO) will approve or disapprove such requests "prior to contract award." Enabling the DoD CIO to issue a decision at any time "prior to contract award" may complicate procurements. For example, an otherwise responsive offeror may be deemed non-responsive or not responsible at the final hour when neither the offeror nor the agency has time to address the issue through discussions and/or an amended proposal. This may impact DoD's ability to obtain the best value, especially where the requesting contractor or subcontractor could have fully implemented the NIST SP 800-171 requirements with adequate notice.

CODSIA recommends that the policy and clause include a set time limit for the CIO or their authorized representative to approve or disapprove deviation requests from offerors. As currently stated in the interim rule, decisions on such requests are not time-bound, so could go unaddressed for any length of time. As pressure builds from companies seeking deviations to the NIST 800-171 controls to be responsive to acquisition requirements, the written requests could become overwhelming and the lead-time for awards could drag well beyond the short time period contemplated in the interim rule. CODSIA thus recommends a notional 3-5 day, or other reasonable period be used to time-bound determinations to the alternative process and/or, in the alternative, that any deviation request unanswered after 10 business days be presumed to be approved by the agency CIO.

It is also unclear from the clause whether, and to what extent, requesting a deviation may impact the evaluation of proposals. The clause should state that agencies shall not downgrade technical proposals, or otherwise penalize offerors, for requesting and/or being granted deviation authority. Otherwise, the allowance for deviations could exist in name only, and the safeguarding requirements could become a barrier to market entry, a result that would be inconsistent with the interim rule's intent. It is also unclear from the clause if subcontractors should request deviations directly or through the prime contractor and what, if any, role the process includes for the prime contractor.

The clause prescription seemingly requires contractors to request a deviation every time a proposal is submitted. This transaction-specific requirement places an inordinate strain and burden on both the DoD CIO and contractors/subcontractors. It would be more efficient and economical to allow contractors to receive a blanket approval of their systems at the enterprise or business unit level that would apply across many contracts with DoD for a specified period of time. This would reduce the transactional and compliance burden on the DoD CIO and afford contractors assurance as to whether or not their request for deviation will be granted in advance of proposal submission and provide some predictability to contractors investing bid and proposal funds into federal competitions. The Department

should further contemplate a "pre-approval' or certification of compliance for vendors that voluntarily wish to seek approval in advance of seeking DoD contract work. Such a mechanism would further reduce the burden on the Department and companies in the DIB, as they could seek and receive approval prior to use of the deviation.

It is also unclear what factors will be considered by the DoD CIO when processing requests for deviation and developing and issuing guidance on any single factor or set of factors would be helpful to ensure consistency across all applications and transactions. Providing such guidance would enable contractors to better prepare their requests and would establish reasonable parameters for contractors, subcontractors, and the DoD CIO to observe. In particular, and unless an exemption for commercial and COTS supplies and services is implemented as requested above, the interim rule should specifically consider the extent to which commercial item contractors with information security systems that are consistent with industry standards will be evaluated.

Finally, it is unclear why DFARS 252.204-7008 and 252.204-7012 are separate clauses? DFARS 252.204-7008 requires compliance with DFARS 252.204-7012, except to the extent an authorized representative of the DoD CIO approves a deviation. Any deviations from the requirements set forth in DFARS 252.204-7012 should occur in DFARS 252.204-7012 to ensure that they apply to the requirements in that clause.

f. Mandatory Cyber Incident Reporting

New reporting procedures significantly increase both the number of possible information systems where contractors and subcontractors must implement security safeguards, as well as the circumstances in which a contractor and subcontractors must report incidents. The interim rule also creates conflicts with other reporting requirements that must be reconciled prior to finalization. Under the interim rule, a "covered contractor information system'' is an information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information. The interim rule requires reporting of any "cyber incident" that "affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support." A cyber incident that affects the contractor's ability to perform "operationally critical support" could also include incidents on systems beyond "covered information systems" and the interim rule requires reporting of those incidents as well. Furthermore, the breadth of the interim rule has implications for defense contractors whose cyber incidents might involve export control violations. Disclosures to DoD prior to submission of a voluntary disclosure to the U.S. government agency with jurisdiction over the relevant export control regulations could eliminate the penalty mitigation that the agency otherwise would grant to companies that voluntarily disclose their export control violations to the agency.

DFARS 204.7302(b) and 252.204-7012(m)(2) require prime contractors and subcontractors to "rapidly report" cyber incidents to the Government. Subcontractors must also report in the same timeframe to their prime contractor. The clause requires the subcontractor to

provide the prime contractor with the "incident report number, automatically assigned by DoD," but does not otherwise state what information must be provided to the prime contractor. The interim rule, however, does not expand on what constitutes discovery of an incident. Without guidance as to what information must be disclosed, it is unclear whether the subcontractor may be required to reveal proprietary information as part of the disclosure and/or the extent to which the prime contractor is required to maintain the confidentiality of such information. Moreover, the requirement that this information be "rapidly reported" may not allow the private parties time to negotiate a non-disclosure agreement with respect to such information. Alternatively, the clause should limit the prime contractor's use of any disclosed information as the interim rule does with respect to third-party contractors under DFARS 252.204-7009.

This substantially increased reporting requirement will increase operating costs and require additional personnel to develop cyber incident reports and to properly submit those reports to the appropriate agency. We recommend that a threshold be established on when a contractor and subcontractor would be required to report a cyber-incident. The guidance is unclear on what types of incidents require government notification. For example, if a botnet is detected on the network, it is unclear if it is a reportable cyber incident, particularly if no breach of data is detected. The scope of reportable cyber incidents must be more clearly defined and bounded.

In regards to cyber Incident reporting, which states, "The contractor shall send only one report to each agency POC identified in the contracts, not a report for each contract from that agency. The report may contain information required by other agencies, so one report may satisfy the requirements of multiple agencies…" Strict construction of the regulation will result in thousands of reports. We recommend that the agency POC be a centralized figure/office in which all cyber incident reports are submitted to or, in the alternative, a centralized figure/office that handles reporting for all contracts under which a given contractor performs. Incident reporting must be standardized and companies (contractors, subcontractors, commercial entities) need to be able to report once to the government on an incident rather than having to report to multiple DoD components separately. This situation is further exacerbated by the differences between this interim guidance and the draft OMB cybersecurity acquisition guidance, which will only further hamper the ability to implement concise, well understood and standardized reporting requirements.

DFARS 202.7302(d) states that a reported cyber incident is not per se evidence of inadequate safeguards. The section does not, however, state what other factors may be considered in making this determination. For example, may the Government determine a contractor or subcontractor's system inadequate when the contractor/subcontractor makes a good faith effort to implement the requirements of the clause, but is nevertheless the subject of a cyber incident? Establishing a "safe harbor" or providing more detail as to how contractors and subcontractors can comply with the requirements and mitigate risk would help ensure that this interim rule does not create an undue burden or exposure for contractors and subcontractors.

While CODSIA would like to believe, based on DFARS 202.7302(d), that DoD will handle all investigations of cyber-incidents using internal resources, thereby maintaining confidentiality and the integrity of the process, but the interim rule in the next clause references "[s]upport services contractors directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting (e.g., providing forensic analysis services, damages assessment services, or other services…." This language would imply that the DoD plans to outsource its cyber incident investigation function, despite the language in subsection (d) above. Such outsourcing creates a substantial risk of conflict of interest, since many companies that provide forensic analysis services compete with contractors that sell cybersecurity products/services to the government. Even where they do not, such forensics firms may have strategic relationships that would preclude them from being objective in their analysis. CODSIA would reiterate that we prefer there be a separate DoD cybersecurity forensics office established to investigate cyber incidents and if such an office cannot be established, then the interim rule needs to better prescribe protections of information and how to avoid conflicts of interest when using contracted services. Furthermore, when third-party contractors may provide services as described in DFARS 202.7302(e), the interim rule should establish that a reporting company shall have the right to object to the involvement of a particular third-party service provider participating in the investigative process and call to the attention of the contracting officer the conflict of interest that would be the basis for such an objection.

The government should encourage reporting by maintaining confidentiality of all contractor information and reports. But the interim rule leaves too many questions unanswered regarding the protection of reported data to give confidence to contractors. For example, will non-disclosure agreements be put in place for third party companies who receive reported data? Will there be a chain of evidence established with traceability to determine where the reported data was sent and by whom it was accessed? What assurances can the government provide that the data is secure once reported? All of these questions must be addressed before the final rule is promulgated. DoD must be able to protect against unauthorized use or release of contractor information, including contractor attributable or proprietary information and the current construct of the interim rule and the existing DoD protections known to industry do not clearly afford such protections. The Department must provide greater clarity regarding its role and the role of its contractors in the implementation of this policy.

g. Identifying and Marking Covered Defense Information

Identifying controlled defense information will be a significant challenge, as the interim rule does not mandate that DoD identify its own data. Complicating matters is the expansive definition of CDI, which makes it difficult for contractors and subcontractors to identify the same — covered defense information includes essentially any piece of information not in the public domain and must be treated as such and protected under this interim rule. Thus, the interim rule places undue responsibility on contractors and subcontractors to identify and adequately safeguard government information that "would meet" the criteria outlined in DoD Instruction 5230.24, Distribution Statements on Technical Documents, regardless of

whether such information is identified in the contract or on the face of a document as being subject to the restrictions outlined in DoD Instruction 5230.24. This is a departure from the previous treatment of information deemed to be "Unclassified Controlled Technical Information." The previous UCTI rule did not require the contractor to make any independent determinations about whether information "would meet" the guidelines in DoD Instruction 5230.24. Instead, the previous definition required controlled technical information "to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24."

The Department should restore this previous construct and ensure that contractors and subcontractors will not be required to make independent decisions regarding whether information "would meet" the requirements of DoD Instruction 5230.24 or should be marked with one of the applicable restrictive legends. DoD Instruction 5230.24 makes clear that "determin[ing] the appropriate markings" and ensuring "that all technical documents, including research, development, engineering, test, sustainment, and logistics information, regardless of media or form, are marked correctly," is an "inherently governmental responsibility.[3]" Because the responsibility for determining which restrictive legend, if any, should apply to technical information is "inherently governmental," it is unreasonable for the Department to impose a unilateral contract obligation on contractors to treat as "covered defense information" any information that "would meet" the requirements in DoD Instruction 5230.24, even if that information does not bear the appropriate restrictive legend.

If a contractor or subcontractor receives information (either from the Government or a third party) that is not clearly marked with one of the restricted distribution legends (B through F) under DoD Instruction 5230.24, the contractor or subcontractor should have no contractual obligation to determine whether the information "would meet" the requirements in DoD Instruction 5230.24, but for the lack of a restricted marking. Likewise, if the Department expects industry to appropriately safeguard sensitive information, it must clearly identify what that information is, so that contractors and subcontractors are in a reasonable position to know the scope of information to which the "adequate security" requirements in DFARS Clause 252.204-7012 apply.

"Covered Defense Information" has also been expanded to include export-controlled information – but the definition of what is included in this category appears to be broader than information that is controlled by export laws. Contractors and subcontractors will not necessarily be able to determine whether specific information "could reasonably be expected to adversely affect the United States national security and nonproliferation objectives." Rather, that determination should be left to the government by way of the various export laws. We suggest that this section be modified to refer only to export controlled information, and not include a general description of the type of information that

[3] See DoD Instruction 5230.24, Enc. 2 at 9 (emphasis added); see also id., Glossary, defining "controlling DoD office" as "the DoD activity that sponsored the work that generated the technical document for the DoD and has the inherently Governmental responsibility for determining the distribution of a document containing such technical information."

may be subject to export controls. We suggest that this section be re-worded as follows: "Unclassified information concerning items requiring licenses under the export administration regulations, or the international trafficking in arms regulations and munitions list." Presumably sensitive dual use and nuclear technology information that is separately listed would be covered by the EAR or ITAR regulations.

"Covered Defense Information" now includes "Critical Information." The definition of "critical information" included in DFARS 204.7301 and DFARS 252.204-7012 refers to "operations security" and the "Operations Security Process." If DoD is to include this concept in the new definition of Covered Defense Information, given that this clause is applicable to commercial contractors and subcontractors at all tiers, DoD should consider providing more detail and explanation as to what specific information is covered by this provision because commercial entities will not be familiar with this terminology or the process.

h. Contracting for Cloud Services

The Obama Administration and Congress have instituted policies for federal agencies, including DoD, to migrate many functions to the cloud to help modernize their systems, improve security, increase energy efficiency and reduce cost. Consequently, agencies are under orders to close large numbers of legacy data centers to speed up system modernization and increase costs savings. Unfortunately, this interim rule negates cost savings opportunities and other benefits that cloud services may offer and undermines security by adding a physical location requirement of data stored in the cloud environment. It requires cloud-computing service providers "to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all government data that is not physically located on DoD premises." Cloud computing services providers and users of cloud computing services under DoD contracts are all required to report cyber incidents in compliance with the reporting requirements of this interim rule.

With respect to the cloud policy articulated in this rulemaking, it is unclear why cloud computing was appended to this rulemaking, other than a vague connection of all things cyber to federal IT processes and commercial IT business models. Because most federal cloud computing policies are governed under other processes, like the Federal Risk and Authorization Management Program (FedRAMP), the interim rule does not align directly with the other statutory cybersecurity requirements being implemented in this rulemaking. CODSIA thus recommends removing all the 252.239 Cloud Computing policy sections and clauses from this rulemaking and re-publishing them as separate rules.

In the alternative, we recommend clarifying the prescription for application of the cloud computing clauses. The prescription states that the clauses are only required where IT services are being acquired, but the clauses themselves at 252.239-7009 and 252.239-7010 appear to have a broader reach to contracts and subcontracts for other than IT services and appear to require a certification where a contractor or subcontractor plans to use cloud services as an element of their internal performance on a contract or subcontract, but

whose efforts are not specifically for cloud computing services contracts. Given that the DoD has adopted more stringent cybersecurity and reporting requirements in the new DFARS 252.204-7012, we suggest that the interim rule clearly limit the applicability of the cloud computing clauses to those situations where the DoD is acquiring such information technology services from cloud computing services providers for its direct use.

While industry would oppose broadening the scope of coverage, if there is an intention to broaden the representation requirements to all contracts where a contractor or subcontractor uses cloud services for their own purposes unrelated to performing on an IT services contract, the DAR Council needs to clarify that. Otherwise there is a presumption that where not specifically providing IT services to the DoD, a contractor or subcontractor need not make any representation about their use of cloud computing services.

The guidance hampers federal efforts to improve reciprocity of security certifications and accreditations by requiring that cloud computing services contracts can only be awarded to a cloud service provider who has already obtained a Defense Information Systems Agency (DISA) provisional authorization. The guidance fails to address cases where a FedRAMP Joint Authorization Board (JAB) provisional authorization or another agency's Authority to Operate (ATO) has already been attained for a cloud solution. In addition, there is a lack of clarity about how new cloud solutions will be rapidly assessed by DISA in time for the new solution to be awarded a contract with a DoD component. Taken together, these issues seriously hamper federal goals of security reciprocity and making secure cloud solutions rapidly available to the government. The Department should revise the interim rule to accept not only DISA provisional authorizations, but also JAB provisional authorizations and agency ATOs. If all authorizations cannot be accepted, then DoD should revert to the cloud security models governed by the JAB and implemented through FedRAMP as the requirement for cloud computing services under these new clauses.

Section (l) of DFARS 252.239-7010, "Cloud Computing Services," requires prime contractors to flow down the substance of the clause in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items. The majority of the provisions of the clause, however, do not apply to commercial cloud infrastructure (i.e., IaaS) providers because they are outside of the control of those providers. Such an assignment of responsibility and liability would seem to reflect a lack of knowledge regarding cloud provider business models on the part of the regulators. For example:

- 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 prime contractor, the lead systems integrator and/or the managed services provider (the "prime") 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 primes store and process on their infrastructure is

government data, any liability for ensuring that government data stays within the United States.

- 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.

- 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 flowdown to IaaS providers, but to the prime using the cloud.

- 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.

- 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.

Although physical access to infrastructure (e.g., data centers) is within the IaaS providers' control, IaaS providers are unlikely to agree to DFARS 252.239-7010(i)(3), which provides that the government may require physical access to data centers for purposes of audits, investigations, inspections, or other similar 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. The DFARS should be revised to reflect this practice.

Congress has required the Executive Branch to eliminate these types of localization requirements around the world when it passed the 'Bipartisan Congressional Trade Priorities and Accountability Act" in June 2015, otherwise known as the Trade Promotion Authority (TPA). Specifically, this Act states in subparagraph 2)(b)(9):

> *LOCALIZATION BARRIERS TO TRADE —The principal negotiating objective of the United States with respect to localization barriers is to eliminate and prevent measures that require United States producers and service providers to locate facilities, intellectual property, or other assets in a country as a market access or investment condition, including indigenous innovation measures.*

This interim rule will make it far more difficult for the U.S. government to achieve this negotiating objective, since countries maintaining or considering such measures will point to the interim rule as evidence that the United States is practicing what it preaches others should not do.

Furthermore, TPA subparagraph (2)(b)(6) requires the Executive Branch to prevent other governments from implementing measures that restrict cross border data flows, including requirements to store or process data locally:

> *DIGITAL TRADE IN GOODS AND SERVICES AND CROSS-BORDER DATA FLOWS — The principal negotiating objectives of the United States with respect to digital trade in goods and services, as well as cross-border data flows, are— (A) to ensure that current obligations, rules, disciplines, and commitments under the World Trade Organization and bilateral and regional trade agreements apply to digital trade in goods and services and to cross-border data flows; (B) to ensure that— (i) electronically delivered goods and services receive no less favorable treatment under trade rules and commitments than like products delivered in physical form; and (ii) the classification of such goods and services ensures the most liberal trade treatment possible, fully encompassing both existing and new trade; (C**) to ensure that governments refrain from implementing trade-related measures that impede digital trade in goods and services, restrict cross-border data flows, or require local storage or processing of data***;*** (emphasis added).

From our perspective, this interim rule flies in the face of the stated intentions of Congress regarding forced data localization and that negotiating objective.

Fundamentally, localization policies such as this interim rule undermine security practices and the White House's stated position that "requirements to store data or locate hardware in a given location hurt competition, stifle innovation, and diminish economic growth.[4]" Furthermore, security of a service or system is not a function of the geography of a server and the location of data has no bearing on whether the data is secure. These types of requirements are detrimental to innovation, job creation, and economic growth--both locally and globally. Data does not recognize borders. Instead, it crisscrosses the globe through data centers and resides in the cloud, often by design for efficiency or as a safeguard in case of a disaster or technical failure. Restrictions on the movement of data dilute the lifeblood of the global economy. Data localization requirements also lead to increased costs for both companies and the federal government by making the use of local data centers more expensive.

---

[4] https://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence

One recent study by the Leviathan Security Group indicates that data localization requirements can make the server costs of local companies 30-60% more expensive.[5] Such costs will make it very difficult for smaller companies to compete in an extremely competitive procurement environment in the United States, which ultimately would raise costs for the government and for taxpayers. Another recent study has shown that data localization requirements can act as a drag on economic growth.[6] With the U.S. economy still recovering from the economic trauma of the financial crisis, eliminating the data localization requirements in this interim rule from the final rule would be a prudent action, which we would support.

i. Access to Contractor and Subcontractor Systems, Information, and Equipment

The access provisions include separate requirements in the Safeguarding CDI and incident reporting policy and clauses distinct from the cloud computing policy and clauses. With respect to the Safeguarding clauses, the access approach includes providing any "malicious software" discovered, preserving and protecting any relevant media and data for 90 days after the incident report, authorizes DoD access to physical equipment or information needed for forensic analysis, and to provide damage assessment information, as needed and upon request, for DoD to pursue further investigations. The Cloud Computing policy and clauses require many of the same elements for an investigation and analysis, but also require an order of magnitude more access to cloud service providers, including additional records management and physical facilities access.

Cloud service providers, especially those serving multi-tenant environments have been very adept in investigating security incidents without the need for physical access to equipment by the customer. Agreeing to provide such access to DoD would pose an unacceptable risk to the security, privacy and confidentiality obligations of the vendor to other customers and regulators – including other government and DoD customers, jeopardize intellectual property protections, place cloud customer data at unnecessary risk and set a precedent for permitting foreign governments to physically access cloud data centers and seize equipment. The data collection methods prescribed in this DFARS do not fully consider the nature of cloud-based services and are largely ineffective at achieving DoD's ultimate security objectives. Instead, we encourage the DoD to work with the NIST and SRG risk management framework to ensure vendors have the capabilities to perform the right analysis in the case of any security incident and provide customers timely and actionable information.

Finally, the proposed methods present opportunities for leaks of information related to a cloud service provider's physical hardware configuration, data center layout, physical perimeter security, etc., that could lead to exploitation by malicious actors. Given prior U.S.

---

5 https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

6 http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

leaks of sensitive commercial security information, and the sheer number of non-governmental contractors working on behalf of DoD, we have no reason to believe that any physical access requirement could be paired with an adequate level of assurance that such information will not fall into the wrong hands. DoD appears to be following existing investigative models designed for access to physical products and manufacturing environments to inform their access policies to investigating cyber-security breaches, with an approach to access facilities, information and people not always representative of a physical storage space or tangible media in all instances. CODSIA recommends that DoD work with industry to determine a set of feasible forensic analytic policies and techniques that recognize that information and/or facilities may not be physically located within the jurisdiction or control of the DoD or their agents. Additionally, access to people and information should follow existing oversight protocols embedded in the FAR and DFARS and not attempt to reinvent new and onerous investigation protocols for cyber-security.

If DoD takes possession of physical media or contractor/subcontractor owned equipment or information for the purpose of forensic or investigative reasons, there should be a complete and thorough accounting of that action, and an inventory of such materials kept by both the DoD and the contractor/subcontractor. DoD should be required to return or reimburse the contractor or subcontractor for such resources at some reasonable time after the incident report investigation is concluded, commensurate with the facts governing the incident or breach. DoD should also be held responsible for the value of any such impounded equipment, media or information should those resources be temporarily or permanently confiscated from the contractor or a subcontractor, due to no failure of the contractor/subcontractor to meet the requirements of the clauses and regardless of the conclusions about the root cause of the breach.

The provision regarding access to additional information or equipment necessary for forensic analysis in subsection (f) requires contractors to "...provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis." CODSIA would recommend modifying this clause to state: "…upon request by DoD, the parties shall discuss in good faith whether additional information or equipment is necessary to conduct a forensic analysis."

Other Concerns

Impact on global business and non-federal clients

There is already a strong global backlash against industry (to include, but not limited to companies in the aerospace, defense, information and communications technology sectors) because of a perception that the U.S. government, through the National Security Agency (NSA), has access to contractors and subcontractors networks. Such a condition will only be exacerbated by the finalization of this interim rule. Governments around the world closely watch U.S. policies, and a U.S. requirement that would discriminate against a vendor based on its relationship with a foreign country (or government) could embolden other governments to enact similar restrictions as a condition of sale into their own markets. Such

an eventuality is particularly concerning, and perhaps even likely, given the heightened suspicion and scrutiny many foreign governments are focusing on U.S-based companies in light of the Snowden revelations and stories about U.S. corporate "collusion" with the U.S. government. In fact, governments already are enacting or proposing policies that are causing U.S. firms to be shut out of foreign markets and requiring unfettered access to company's facilities may only serve to fan those flames. Companies have to sign agreements certifying that the U.S. government does not have access to their networks (i.e. the German No-Spy Declaration, imposed by the German government in mid-2014), which create international impediments to compliance with this interim rule for many companies.

Sharing and protection of contractor and subcontractor data and information

DFARS 204.7302(c) recognizes that the disclosure of the required information may cause substantial competitive harm to contractors/subcontractors and requires the government to "protect against the unauthorized use or release of information that includes contractor attribution/proprietary information." DFARS 252.204-7012(h) contains requirements for the government's safeguarding of such information. While these clauses recognize the importance of protecting proprietary information, they do not *ensure* protection or establish minimum requirements for protection. For example, the interim rule does not afford contractors and/or subcontractors an opportunity to review a proposed disclosure or distribution (e.g., to Government entities conducting counterintelligence or law enforcement investigations, entities assisting with diagnosis, detection, or mitigation, support service contractors, etc.) before it is made to ensure that proprietary information is not being inadvertently or unnecessarily released. This omission from the interim rule is especially problematic because the interim rule provides that information may be disclosed outside the government including to "entities with missions that may be affected by such information." The interim rule also does not provide how the government will maintain the information to ensure that it is secure. The sharing of sensitive and proprietary company data with third parties is particularly problematic and must be resolved. In addition, limitations on access to equipment that may also be used by non-government customers or for other internal company uses must be addressed. We recommend that DoD add a requirement for third parties to sign a non-disclosure agreement (NDA) with each company they may conduct forensics or an investigation against. The systems they are reviewing may have personally identifiable information (PII), proprietary proposal data, corporate proprietary labor rates, salary information or proprietary pricing information, for example. Signing a NDA would provide each company with another level of protection not currently provided in the interim rule.

Further, the DFARS 252.204-7012(h) contains a marking instruction which is impractical in the context of the timing of the reports, as well as to the preservation of evidence needed to conduct the cyber incident reporting. For instance, marking of an image required under DFARS 252.227-7012(h) would seemingly be contrary to the purpose of producing the image. Thus, all documents related to the cyber incident report and investigation should be deemed marked and usage specifically restricted to the investigation and reporting set forth in DFARS 252.204-7012.

Under DFARS 252.204–7012(i), the Government can share this information with a contractor, as long as the contractor has DFARS 252.204–7009 in their contract. DFARS 252.204–7009, however, lacks the protections normally afforded to contractors and subcontractors where sensitive information is provided to covered government support contractors under DFARS 252.227-7025, including the right to require a NDA, which is the norm in DoD contracting and is codified in 10 U.S.C. 2320(f)(2). To the extent such contractors and subcontractors are not covered government defense contractors, such required sharing is in apparent contradiction with 10 USC 2320, as implemented in DFARS 252.227-7013 and 252.227-7014 for data included in a CDRL. It is not clear what the statutory basis is for not following established DoD contracting norms set forth in 10 U.S.C. 2320(f)(2) and DFARS 252.227-7025 and there is no support in the interim rule comments that having at least these same protections in DFARS 252.204–7009 would substantively prevent the Department from completing the cyber report in a timely fashion. Having such protections is also important in ensuring that sub-tier and/or commercial suppliers will accept this clause in their contracts, since the use of NDAs is customary in the commercial marketplace for protecting matters under investigation. Therefore, while the Section recognizes that there may be a need to ensure that contractors can receive cyber incident reports and aid in the investigation of cyber incident reports, CODSIA believes that the provisions of DFARS 252.204–7009 need to be brought into line with the DoD contracting norms set forth in 10 U.S.C. 2320(f)(2) and DFARS 252.227-7025 to ensure protection of the sensitive information released in a cyber incident.

Lastly, while this information may include competitively sensitive contractor information; the government apparently has no clear obligation to protect this information, except for information that is provided to support contractors. Paragraph (j) addressing contractor (and subcontractor) attributional/proprietary information further permits disclosure "for any other lawful government purpose or activity" subject to all applicable statutory, regulatory and policy-based restrictions on the use and disclosure of such information. That condition is extremely vague and, given that such sensitive attributional and/or proprietary information may be broadly disclosed, does not provide sufficient protection. Rather, for each disclosure of any information that is provided in response to the government's request following a reported cyber incident, the government should contractually bind non-government entities to whom it discloses the information to use such information only for the specified purpose, and not to disclose it to any third parties without the disclosing contractor's or subcontractor's consent. For disclosures to other government entities, the government should also be required to ensure that such agency understands the sensitivity of the information and to mark it is some manner that indicates that it is subject to any relevant and controlling statute, i.e., the Trade Secrets Act, 18 USC 1905, the Economic Espionage Act and Executive Order 12600, etc., and is not subject to disclosure under FOIA.

Liability Protection for Information Disclosures pursuant to the interim rule's reporting requirement

Section 1641 of the FY16 NDAA (Conference Report version) changes Chapter 19 of Title 10 to create statutory protections from third party liability for cleared defense contractors and operationally critical contractors, as those terms are defined in the statutes and in this rulemaking. The statutory protections apply to any dissemination of information made per specified DoD procedures by cleared defense contractors and operationally critical contractors to meet the interim rule's incident reporting requirements, and apply broadly to all reports and for any cause of action, except for a contractor's willful misconduct in the reporting of that information.

The interim rule contains a proposed clause (252.204-7009, Limitations on the Use or Disclosure of Third Party Contractor Reported Cyber Incident Information) that limits use or disclosure of reported incident information by third party DoD support service contractors that might have access by virtue of their contract obligations related to safeguarding covered information or incident reporting. The clause restricts unauthorized use by the third party contractor and establishes remedies for breach of those duties including authorizing civil actions by the party or parties originally reporting the incident.

While this remedy applies where a third party breaches their contractual non-disclosure duty, none of the proposed clauses provide for any of the liability protections envisioned in Section 1641 and DoD must consider aligning those protections in the final rule alongside the third party restrictions to establish a legal framework offering safe harbors from liability to those reporting in good faith and punishes those that breach their duty not to disclose relevant non-public information. Considering that Congress has clearly indicated its intent to provide broad liability protection for those classes of contractors, the interim rule should be amended in final form to include a provision in 252-204-7012, Safeguarding Covered Defense Information and Cyber Incident reporting, incorporating those statutory liability protections. The interim rule should also be amended to afford proper liability protections as a result of the flowdown requirements, applying to subcontractors and those subcontractors that sell commercial parts and services to the Department.

Reconcile requirements with Sec 325 of Intelligence Authorization Act of FY14

This interim rule does not reconcile its requirements with those that will be imposed on defense contractors that are also subject to the requirements imposed by section 325 of the Intelligence Authorization Act of FY2014. The Department needs to include procedures in this interim rule on how cleared defense contractor and intelligence contractors and their subcontractors will submit a single report that satisfies the requirements of both the IC and DoD.

OMB Draft Guidance on Improving Cybersecurity Protection in Federal Acquisitions

Currently, there are a number of inconsistencies between the DoD interim guidance and the draft OMB cybersecurity acquisition guidance.

Among other things, the draft OMB guidance contained proposed reporting requirements for agencies to require in their acquisition processes; these agency processes are still in flux, but industry made several recommendations regarding differentiating between reporting requirements for contractor systems operated for the government and for contractor internal IT systems with incidental levels of CUI, insuring a single reporting process, observing necessary protocols for release and disclosure to third parties (addressed also herein), and addressing liability and indemnification issues (also addressed in detail herein). These two sets of guidance must be reconciled to avoid disparate reporting requirements, conflicting compliance regimes, competing security requirements and other unnecessary costs that will have to be borne by contractors and subcontractors and passed along to taxpayers in the final pricing for goods and services. We request that these conflicting requirements be resolved before cybersecurity requirements become fragmented and we lose the gains created by establishing consistent controls and reporting requirements across the entire federal government.

We recommend that DoD align with and leverage the OMB guidance to alleviate the possibility of additional contractor and subcontractors reporting requirements and build some predictability and consistency into a government-wide reporting process. This will also address the confusion for the large number of companies who do business with multiple federal agencies.

Impacts to Small Businesses

This interim rule applies universally to all DoD suppliers, including small businesses (SBs). While some SBs can comply with the basic safeguarding clause in place now, as stated above, the new requirements will create an immediate compliance burden that many SBs cannot afford to instantly mitigate, either as primes or as subcontractors. CODSIA recommends that the Department consider alternatives for SBs to meet the compliance requirements, or establish a phased-in implementation and a new Class Deviation as stated earlier in this letter. Without such alternatives, DoD will lose many of the SBs in their current portfolio because they will be instantly out of compliance. Furthermore, without such an accommodation, DoD will certainly lose the edge with enticing new and innovative SBs to build innovative and agile procurement frameworks.

DoD Oversight

A significant unresolved issue is how the DoD will conduct oversight of contractor performance and the systems identified throughout the operative clauses. The DCMA have posited that they do not currently have the capability to oversee contractor IT systems and cyber-security compliance. Since enforcement of the clauses is a huge part of this policy, CODSIA recommends that an enforcement agent or agents capable of performing contract oversight be identified or proposed by DoD prior to any final rules, and in concert with industry views, so that industry can evaluate the costs and processes needed to engage with any new DoD oversight entity not heretofore involved in quality or contract surveillance activity.

Conclusion

In conclusion, CODSIA requests that the Department suspend implementation of the interim rule pending addressing the significant issues we raised in these comments and immediately implement the broader class deviation discussed above to allow phase in and tailored compliance for some period. We further recommend that the Department establish a 2-year transition period for any contract entered into before January 2016. We also request again that the Department host a public meeting or use some type of public discourse mechanism (akin to the GSA Interact portal), to respond to contractors and subcontractors questions and concerns for implementing these requirements. These requirements are burdensome and have an impact beyond government contracting and therefore necessitate a robust dialogue with the impacted community prior to finalizing this interim rule. .

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, who is serving as the CODSIA Case Manager. Pam can be reached at 202-626-5725 or at pwalker@itic.org.

Respectfully submitted,

Rusty Rentsch
Assistant Vice President
Technical Operations & Workforce
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

Will Goodman
Vice President for Policy
National Defense Industrial Association

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

Alan Chvotkin
Executive Vice President & Counsel
Professional Services Council

Appendix:
Questions for the Record

In a recent CODSIA meeting with the Office of Defense Procurement and Acquisition Policy (DPAP), it was noted that a public website would be created to answer many of the most frequently asked questions posed by industry. We offer the following questions for inclusion in this activity and encourage the Department to publish this website with answers as soon as possible, as contractors and subcontractors continue to struggle with implementation.

- Clarify how or whether the term "operationally critical" applies to contractors/subcontractors; "Operationally Critical Support" – this definition indicates that the Government will designate which supplies or services are critical for airlift, etc., but it does not indicate where such information will be found. Will it be included in the contract itself if this is relevant? If not, where would a contractor or subcontractor find this information? Again, commercial suppliers will not have any familiarity with where to find such information.

- Can the Department describe their capabilities to process requests for additional information and access to equipment to conduct forensic analysis? Industry has adopted standards and protocols that must be followed for investigation, collection, preservation, and analysis of data or evidence regarding an incident or threat. Will Industry be able to support and adhere to those standards and protocols and if so, how? For example, it is not clear how industry can establish and maintain a clear line of forensics chain of custody when information or equipment must be provided externally to the Department?

- What are the reporting procedures related to each role (the Department, the Department's Cyber Crime Center, DIBNET Portal, contractor, subcontractor)? Will the prime contractor be provided alerts when an incident report is submitted to the Department and will the reports be shared with the prime?

- What forms of "adware" are of concern per the "Malicious Software" definition includes "*some* forms of adware". Can the reference be clarified, as there clearly is adware that is not malicious?

- What is the submittal and approval process for alternate security measures and deviations from NIST 800-171, and will evaluation criteria and approval schedule timelines be included as part of the information about that process? How will the Department communicate the approvals or disapprovals? Will only the requestor be informed? Will there be an authorized representative of the Department's CIO to make these decisions? Further clarification is needed on how the Department expects contractors or subcontractors to conduct their self-assessment of existing cyber systems against the high-level requirements of 800-171? Does the Department offer any

mechanism for companies to present their self-assessment, or to seek the Department's assessment, in order to assure compliance? Or, will the Department be content to rely upon contractors or subcontractors to self-assess and then to evaluate compliance only after a cyber event?

- Why has the Department decided that it would invoke all the families (basic and derived) of requirements in NIST 800-171 rather than selecting some? Also, if the Department's components conclude that the impact to certain data is greater than "moderate," does the Department anticipate that "higher level" controls than those in NIST 800-171 will apply? How will this be done?

- What is the correlation between Controlled Unclassified Information (CUI) and Covered Defense Information (CDI)? What guidance has been provided for primes and subcontractors to identify the categories of controlled technical information, critical information (operations security) and any other information otherwise identified as it relates to the "op sec" category of "Controlled Defense Information?" Under what circumstances would contractors or subcontractors have the responsibility to mark information if the government customer did not mark the information? Is there a mechanism to query or to confirm a marking decision? Will guidelines be provided similar to export control-handling procedures (i.e., International Traffic in Arms Regulations and Export Administration Regulations)?

- Does (1)(ii) ("[c]ollected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract" include any information provided by the DoD in seeking commercial support and maintenance services? If so, then this would require commercial providers to stand up a completely separate and restricted support and maintenance system for use by the DoD – potentially costing millions of dollars. To avoid this possibility, commercial companies may insist – as part of their support and maintenance terms – that the DoD agree that it will not transmit CDI in seeking support and maintenance services.

- The DFARS references application of other security measures in addition to providing adequate security based on a risk or vulnerability assessment. Will the Department voluntarily partner with Industry or require through contract language that a contractor or subcontractor participate in a CDI risk analysis and assessment to determine the adequate measures and related cost for implementation and operation?

- How does the DISA provisional authorization for cloud computing reconcile with the FedRAMP ATO?

- What is the definition of "DoD premises" used in the interim rule? It is unclear whether Department installations or other Department of Defense real property located outside the United States or its outlying areas are considered Department of Defense premises.

- Please provide greater clarity into the scope and intent of the requirement: "The Contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract." "Related to" is unclear and extremely broad. Why has the Department elected to include the cloud provisions with the CDI measures, since the relationship does not appear compelling? Do the new cloud measures impose changed or greater cybersecurity requirements upon cloud service providers (CSPs), and, if so, where? Is the principle purpose of the cloud provisions to assure the government that it knows in advance before any contractor "outsources" or "outplaces" to the cloud, or is this to be a substantive change to set a new or different safeguards requirement? Is this applicable to subcontractors utilizing cloud services or CSPs?

- Do the cloud clauses apply to the Department's information per the objective statement in any Department, contractor, and/or subcontractors cloud service provider environment or only Department acquisitions of cloud computing services? Will the Department be able to provide a resource to contractors and subcontractors who seek implementation guidance?

- Why was this interim rule introduced in an interim status, effective immediately when the regulators had the direction to address these challenges for years? The interim rule states that this "is necessary because of the urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors." Cyber attacks against federal contractors and subcontractors are nothing new – they have been going on for years. Indeed, the DoD recognized this fact in 2011 when it proposed rules to regulate all Controlled Unclassified Information (CUI). Subsequently, the Department narrowed the scope of the proposal to the UCTI DFARS finalized in November 2013 (which had a similar cyber-reporting obligation and audit right).

- The definition of "covered defense information" includes information "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." Does this sub-category of information include information/documents that are created in the course of providing commercial professional services or support and maintenance services? If so, then the Department is requiring that it be treated differently than commercial customers when procuring commercial products/services – contrary to FASA, FARA and FAR Part 12. Please clarify.

- With the recent spate of high-profile government agency hacks, how can industry be assured that the DoD will be able to safeguard information? What recourse will contractors and subcontractors have if the DoD fails to safeguard such information?

- Is the contracting officer the most qualified individual to investigate a cyber incident, even with assistance from the DoD component CIO/cyber security office? Should there be a separate DoD cybersecurity forensics office established to investigate cyber incidents?

- Does the DoD intend to establish a voluntary disclosure obligation for CDI similar to that for ITAR-controlled information? If so, there is no infrastructure for such scenario in place.

- It is not clear from the interim rule which standards to apply to determine whether an item is "covered defense information." Where it is not clear whether information constitutes covered defense information, what is the process for obtaining clarification from the government? Moreover, what is the process for determining whether information is "critical information" under the Operations Security process? The addition of Operations Security and other regulatory requirements generalized into broadened categories (i.e. CUI, PII, and EXIM) through conflicting laws and regulations will introduce operational inefficiencies and baseless redundancies. Any process should be appropriately centralized to ensure that information is treated consistently across contracts and DoD entities. Further, what standard is applied to determine whether a contractor/subcontractor reasonably complied with the interim rule when determining whether specific information falls within the requirements?

- How complete will the report required within 72 hours need to be? It takes more than 3 days to gather the requisite details, not to mention providing appropriate communications and internal notifications.

- In addition, why are DFARS 252.204-7008 and 252.204-7012 separate clauses? DFARS 252.204-7008 requires compliance with DFARS 252.204-7012, except to the extent an authorized representative of the DoD CIO approves a deviation. Any deviations from the requirements set forth in DFARS 252.204-7012 should occur in DFARS 252.204-7012 to ensure that they apply to the requirements in that clause.

- Does "use of computer networks" include mobile devices connected to a network through applications such as Outlook or webmail?

- If a company was compliant with the 2013 DFARS safeguarding requirements (252.204-7012), how compliant are they with the 2015 version released on August 26? Based on Table D of the NIST 800-171 document, if a company is fully compliant and had implemented all 60 NIST 800-53 required controls from Table 1 in the November 2013 DFARS clause:
    - The company would fully meet 39 of the NIST-171 requirements
    - The company would partially meet 22 of the NIST-171 requirements
    - The company would have 48 new requirements to deal with
    - The net – 64% (70 of 109) of the requirements detailed in NIST 800-171 are new or "partially" new as compared to the NIST 800-53 controls required by the 2013 DFARS clause (252.204-7012). These new and/or partially new requirements require interpretation, assessment and possible implementation in order to ensure compliance.

- If a company chose to continue to use NIST 800-53 controls as the basis for meeting the requirements in NIST 800-171, how many more or less NIST 800-53 controls would be required as compared to the 2013 DFARS requirements (252.204-7012)? Our research shows that the 2013 DFARS requirements (252.204-7012) required the implementation of 60 unique NIST 800-53 controls. Using NIST 800-53 controls to satisfy the 109 requirements from NIST 800-171 would require the implementation of 125 unique NIST 800-53 controls. The net number of NIST 800-53 controls required more than doubled from 2013 to the August 2015 DFARS clause (252.204-7012) release.

- DFARS 252.204-7012(b)(1)(i)(A) states that cloud computing services operated on behalf of the Government are subject to clause 252.239-7010. If a prime contractor is using cloud computing services – e.g., storing covered defense information or running applications involving covered defense information in a cloud infrastructure – in furtherance of a Government contract, but not as "part of an IT service o[r] system operated on behalf of the Government," is the prime contractor required to flow down only DFARS 252.204-7012 to the cloud provider, or both DFARS 252.204-7012 and 252.239-7010? If both DFARS 252.204-7012 and 252.239-7010 must flow down, aren't those provisions duplicative?

- If a prime contractor flows down 252.239-7010 to a cloud services provider pursuant to section (l) of that clause, can the prime contractor and the cloud services provider agree that complying with certain requirements of the clause – such as maintaining all Government data in the United States or outlying areas, and reporting cyber incidents through DIBNET – are the responsibility of the prime contractor as the party managing the cloud services and the applications running in the cloud infrastructure?