IT Alliance for Public Sector
A Division of ITI

September 30, 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

Dear Mr. Pitsch,

On behalf of the Information Technology Alliance for Public Sector ("ITAPS"),[1] a division of the Information Technology Industry Council (ITI), I am writing to you today concerning the Defense Federal Acquisition Regulation Supplement (DFARS) interim rule, Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018). The following request is offered in response to the notice for public comments issued by the Department of Defense (the Department) originally published in the *Federal Register* at 80 FR 51739 on August 26, 2015. Due to the complexities of this interim rule, ITAPS humbly requests that a public meeting be scheduled before the public comment period ends on October 26, 2015, and if that request is granted that a 30-day extension to the comment due date also be considered to adequately provide the public with enough time to respond to this important interim rule.

During the initial calls with our members to discuss and digest the interim rule, we came to the conclusion that there are many unanswered questions and gaps within the rule that complicate our ability to provide a cohesive public comment. We believe that a public meeting could provide the appropriate opportunity for the government to communicate their intentions with the rule and help to address answers to the following questions.

Incident Reporting

1. 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?

2. 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?

[1] **About ITAPS**. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAlliancePS.

3. 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 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 to self-assess and then to evaluate compliance only after a cyber event?

4. 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?

5. 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 have the responsibility to mark information if the information was not marked by the government customer? 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)?

6. 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 participate in a CDI risk analysis and assessment to determine the adequate measures and related cost for implementation and operation?

Contracting for Cloud Services

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

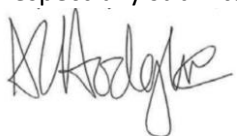
8. What is the definition of "DoD premises" used in the interim rule? It is unclear whether Department installations or other Department of Defense real property located outside the United States or its outlying areas are considered Department of Defense premises.

9. 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 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 cloud, or is this to be a substantive change to set a new or different safeguards requirement?

10. 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 who seek implementation guidance?

We again thank you for the opportunity to offer our input on the matter and sincerely request that the Department host a public meeting on this topic before the public comment deadline. We also request that an extension to this request be granted so that the public may incorporate what they have learned through the public meeting dialogue into their public comments and generate better quality feedback to the Department.

Respectfully submitted,



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