MSPs for the Protection of Critical Infrastructure
2 Parade Street
Huntsville, AL 35806

March 17, 2025

RE: Comments on Federal Acquisition Regulation: Controlled Unclassified Information; FAR Case 2017-016, Docket No. 2017-0016, Sequence No. 1 | RIN 9000-AN56

Consolidated comments and input from the Managed Service Providers making up

MSPs for the Protection of Critical Infrastructure is a 501(c)6 dedicated to informing the U.S. government and critical infrastructure sectors on topics related to the intersection of managed service providers and managed security service providers and national security.

We are thankful for the opportunity to submit comments to help in the pursuit of strengthening national security and bolstering secure, functioning, and resilient critical infrastructure.

Issue: Lack of information and requirements for External Service Providers

Recommendation:

1) We recommend that the rule adopt the same definition for External Service Provider as 32 CFR 170.4(b) “External Service Provider (ESP)”:

   - *External Service Provider (ESP)* means external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization.

2) We also recommend that the rule adopt the same ESP requirements expressed in 32 CFR 170. Specifically, that the use of an ESP, its relationship to the offeror, and the services provided need to be documented in the offeror’s system security plan and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the offeror and ESP with respect to the services provided.

Rationale:

The proposed rule addresses requirements for Cloud Service Providers (CSPs) but does not define or address requirements for External Service Providers (ESPs) including Managed Services Providers (MSPs) and Managed Security Services Providers (MSSPs). ESPs have a significant role in the Federal Contractor Base and ecosystem. The vast majority of the Federal Contractor Base (especially small entities) leverages ESPs to deliver IT Services including management of networks, servers, cloud platforms, endpoint devices, IT service desks, Network Operation Centers (NOCs), Security Operation Centers (SOCs), and many other aspects of their day-to-day operations.

As such, these ESPs have access to and management of Federal Contract Information, Controlled Unclassified Information, Security Protection Data as well as full control of the security of a contractor's IT infrastructure. It is imperative that the FAR Council recognize the importance that ESPs have within the Federal Supply Chain and their role in controlling cost for the ecosystem, but also the potential risk that they can introduce due to their privileged access and management of such a large swath of the supply chain. The FAR Council must identify appropriate standards for ESPs who are maintaining, administering and supporting the infrastructure of organizations handling FCI and CUI data.

Issue: 8-hour reporting deadlines aren't feasible

Recommendation:

We recommend that the rule adopt a 72-hour reporting period for all situations in which an 8-hour reporting period is proposed. This includes both reporting "CUI Incidents" and reporting notifying the government of mismarked or unmarked CUI in conflict with SF XXX.

Rationale:

Specifying a reporting timeframe that does not match existing regulations creates a burden on entities of all sizes and disproportionately impacts smaller entities without the resources juggle competing requirements. Additionally, small entities do not have the resources to support unreasonably short reporting periods. As the rule states, "The new FAR clause is modeled after the most recent version of the clause at DFARS 252.204-7012, which introduced many of these compliance requirements on defense contractors and subcontractors in 2015 and required compliance not later than December 31, 2017." The 72-hour reporting requirement has worked successfully in the Defense Industrial Base for years. Nearly 75% of the DIB consists of small entities. Therefore, the rule ought to leverage the same requirement.

Issue: The definition of CUI incident creates an infinite reporting burden

Recommendation:

The definition of CUI Incident should be changed to:

"CUI Incident means confirmed improper access, use, disclosure, modification, or destruction of CUI, in any form or medium."

Rationale:

Extending CUI Incidents to include any "suspected" improper access, use, disclosure, modification, or destruction of CUI, in any form or medium creates an unreasonable burden because there is no limit on "suspected" incidents. Reporting suspected incidents would result in the requirement to report any activity that might ultimately turn out to be a false positive. This would be a phenomenal waste of time and resources by both government and industry. The cost estimates in the proposed rule do not account for this impact.

Additionally, the use of the term "suspected" in both the CUI incident definition and the reporting requirement is confusing. Taken literally, if a contractor suspected that they suspected there was improper access of CUI, they would need to report. This is not clear. Since CUI incidents include suspected breaches, what is a "suspected CUI incident" intended to include that is not already included in "CUI incident"?

Issue: The threshold for meeting the FedRAMP moderate baseline is unclear.

Recommendation:

We recommend that the rule clarify what it means to "comply … at no less than the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline" by requiring that a CSP be "Authorized" at the FedRAMP Moderate level and listed in the FedRAMP marketplace. The FAR Council should also consider the use of FedRAMP moderate "equivalency" per 48 CFR 252.204-7012(d):

"If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline."

Rationale:

Simply stating that contractors must "Ensure that, if the Contractor uses a cloud service provider to store, process, or transmit any CUI identified in SF XXX

1) The cloud service provider meets security requirements established by the Government for the FedRAMP Moderate baseline" is not clear. "Meets" the security requirements could be construed to mean everything from self-attestation, self-certification, all the way up to full FedRAMP authorization. Self-attestation is not a reliable mechanism for cybersecurity assurance and should not be the basis for federal policy.

Issue: The specification of NIST SP 800-171 revision 2

Recommendation:

We recommend that the FAR Council tightly coordinate future rulemaking efforts with the Department of Defense and their efforts to revise 48 CFR 252.204-7012 and 32 CFR 170.

Rationale:

Harmonizing acquisition regulations across the FAR and the various FAR supplements is critical to preventing contractors from being required to implement, maintain, and sometimes undergo 3rd-party assessment for multiple revisions of NIST SP 800-171 and NIST SP 800-172.

As the various acquisition regulations evolve over time to specify NIST SP 800-171 revision 2 and beyond it is critically important to harmonize the chosen values for "Organizationally Defined Parameters" (ODPs). Failing to synchronize values for ODPs will result in a tremendous burden on all entities, especially small entities with few resources.

Issue: The lack of a 3rd-party assessment requirement

Recommendation:

We recommend that the rule require contractors to undergo 3rd-party assessment to verify the implementation of the requirements in NIST SP 800-171 and SP 800-172 as a condition of contract award.

Rationale:

Although the rule states that "the new FAR clause is modeled after the most recent version of the clause at DFARS 252.204-7012, which introduced many of these compliance requirements on defense contractors and subcontractors in 2015 and required compliance not later than December 31, 2017", the FAR Council seems oblivious to the lessons learned by the Department of Defense since 2015. Merely relying on self-attestation and the possibility that the contract workforce will request proof of implementation is a failed policy as documented in DoD Inspector General report DODIG-2019-015, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems" and DODIG-2024-031, "Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks". As those reports have shown, not only do contractors neglect to comply, the contract workforce also neglects to exercise their ability to request proof of compliance.

We could not disagree more strongly with the rationale against requiring "100 percent inspection" provided in the rule: "non-defense contractors have incentive to ensure compliance with the requirements in FAR clause 52.204-XX to avoid liability for breaches of CUI that may result from improperly protecting CUI being handled on the contractor's information system." At this point in the evolution of cybersecurity regulations the burden ought to fall on the government to prove why 3rd-party inspection *isn't* required. Simply claiming that contractors are sufficiently incentivized to comply falls flat when that exact case study has played out in the defense industrial base. The only result has been harm

to the government, the taxpayer, and offerors whose rates honestly and accurately reflect the level of effort required to comply but lose awards to those who cut corners.

The DoD has spent the last several years establishing an assessment ecosystem to facilitate 3rd-party assessments of the exact NIST standards required by this rule. The CMMC ecosystem is live and assessments are commercially available. Without leveraging the CMMC ecosystem the government will have no assurance that its requirements are being met and that Controlled Unclassified Information is being protected.